ID/Locator Separation Technology and Its Implications for Future Network Design

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

A talk given at Huawei Technologies Co., Ltd.
May 9, 2009

These slides and Audio/Video recordings of this talk are at:
http://www.cse.wustl.edu/~jain/talks/in3_hub.htm

About the Speaker

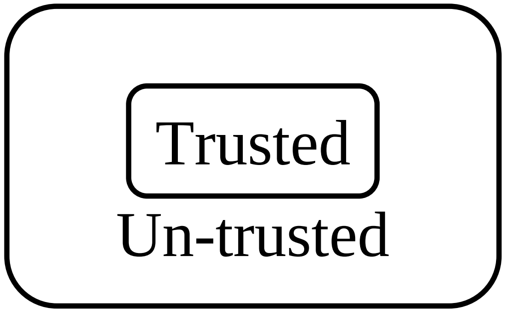
- Fellow of IEEE, Fellow of ACM
- PhD from Harvard University in 1978, over 30 years industry and academic experience in networks.
- Ranked among the top 50 in Citeseer's list of Most Cited Authors in Computer Science
- Co-Inventor of DECbit Congestion management. Variants are now implemented in Frame relay (FECN), ATM (EFCI), TCP/IP (ECN). Every IP packet, every frame relay frame, and every ATM cell has bits resulting from this research.
- ACM SIGCOMM's "Test of Time" award 2006.
- 120+ papers, 7 books, and 100's of contributions to WiMAX Forum, ATM Forum, IEEE, IETF, ANSI, ITU, OIF, and TIA.
- http://www.cse.wustl.edu/~jain/cv_jain.htm

Overview

1. Ten Problems with All-IP Architecture
2. Names, IDs, Locators
3. ID Locator Separation: Key Issues and Implications for Mobile Internet Architecture
4. Our proposed solution: Internet 3.0 and MILSA

Ten Problems with All-IP Architecture

1. Designed for research
   ⇒ Trusted systems
   Used for Commerce
   ⇒ Untrusted systems
2. Control, management, and Data path are intermixed ⇒ security issues
3. Difficult to represent organizational, administrative hierarchies and relationships. Perimeter based.



Problems (cont)

4. Identity and location in one (IP Address)
   Makes mobility complex.

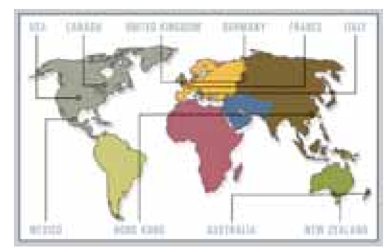
5. Location independent addressing
   ⇒ Most services require nearest server.
   ⇒ Also, Mobility requires location

6. No representation for real end system: the human.

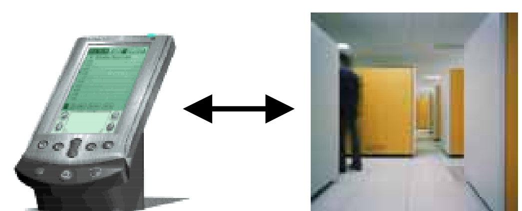
Problems (cont)

7. Assumes live and awake end-systems
   Does not allow communication while sleeping.
   Many energy conscious systems today sleep.

8. Single-Computer to single-computer communication ⇒ Numerous patches needed for communication with globally distributed systems and services.

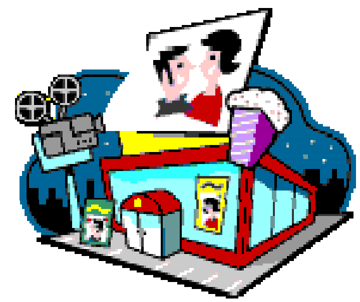


9. Symmetric Protocols
   ⇒ No difference between a PDA and a Google server.



Google

Problems (Cont)



10. Stateless ⇒ Can't remember a flow ⇒ QoS difficult.
    QoS is generally for a flow and not for one packet

Names, IDs, Locators

Name: John Smith

ID: 012-34-5678

Locator:
1234 Main Street
Big City, MO 12345
USA

- Locator changes as you move, ID and Names remain the same.
- **Examples**:
  - Names: Company names, DNS names (microsoft.com)
  - IDs: Cell phone numbers, 800-numbers, Ethernet addresses, Skype ID, VOIP Phone number
  - Locators: Wired phone numbers, IP addresses

A Sampling of ID-Locator Solutions

- **Host Identity Protocol (HIP):**
  - Uses a hash of the host public key as the host ID
  - Solves the host authentication problem
  - No concept of logical and organizational relationships
- **Internet Indirection Infrastructure (I3):**
  - Hash of the ID tells you where to go to find the address
  - The rendezvous server may not be trusted by client
- **Shim6**:
  - Solves the problem of multi-homing
  - Uses one of the IPv6 addresses as identifier
  - Does not handle mobility or security.
- **LISP**, **GSE**, ….

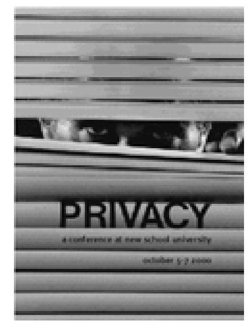
ID Locator Separation: Key Benefits

1. Mobility
2. Site Multi-Homing
3. Traffic Engineering
4. Routing Scalability
5. Device Multi-Homing
6. User Multi-Homing
7. Multi-tiered business models
8. Organizational Policies

Mobility

- **Triangulation**:

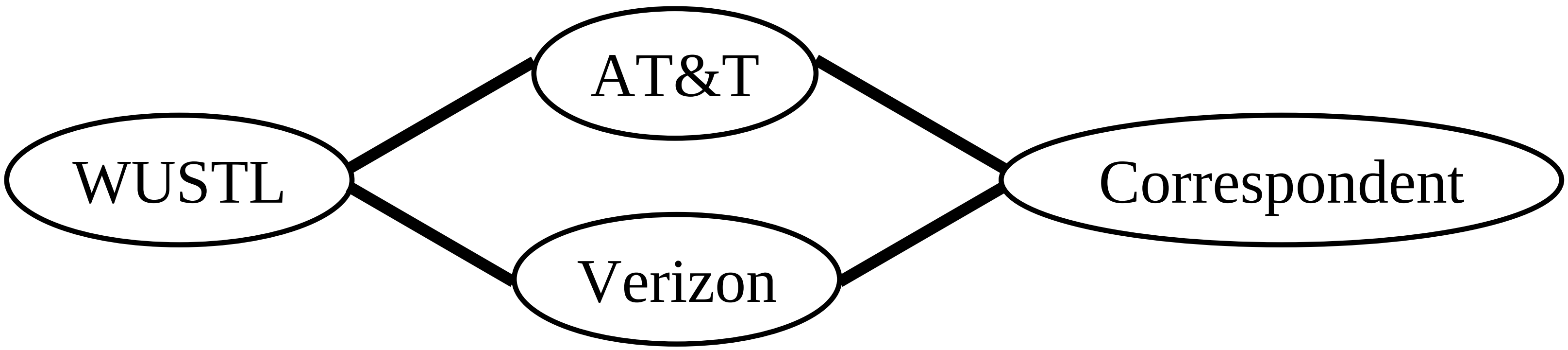
- **Location Privacy**:
  - Mobile locator may not be disclosed to the correspondent



- **Speed**: How fast is the mobile changing location?
  - Slow: Going home and reconnecting
  - Fast: Changing locators (base stations) every few minutes

Site Multi-Homing

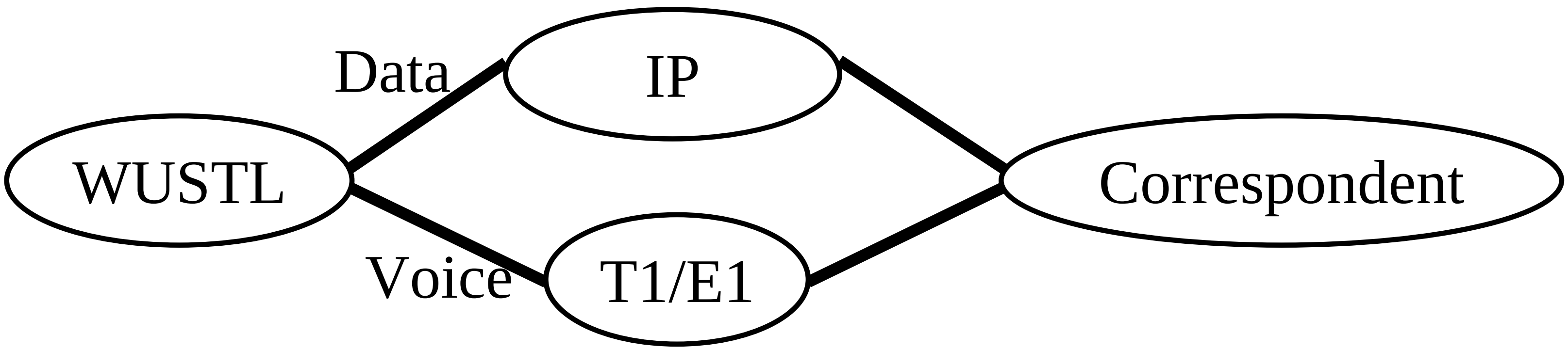
- Multi-homing is not properly represented in current Internet.
  - TCP is bound to an IP address.
    If one port fails, TCP gets disconnected.
- **Site Multi-homing**: Multiple service providers



- Required for fault tolerance (in case one connection fails)

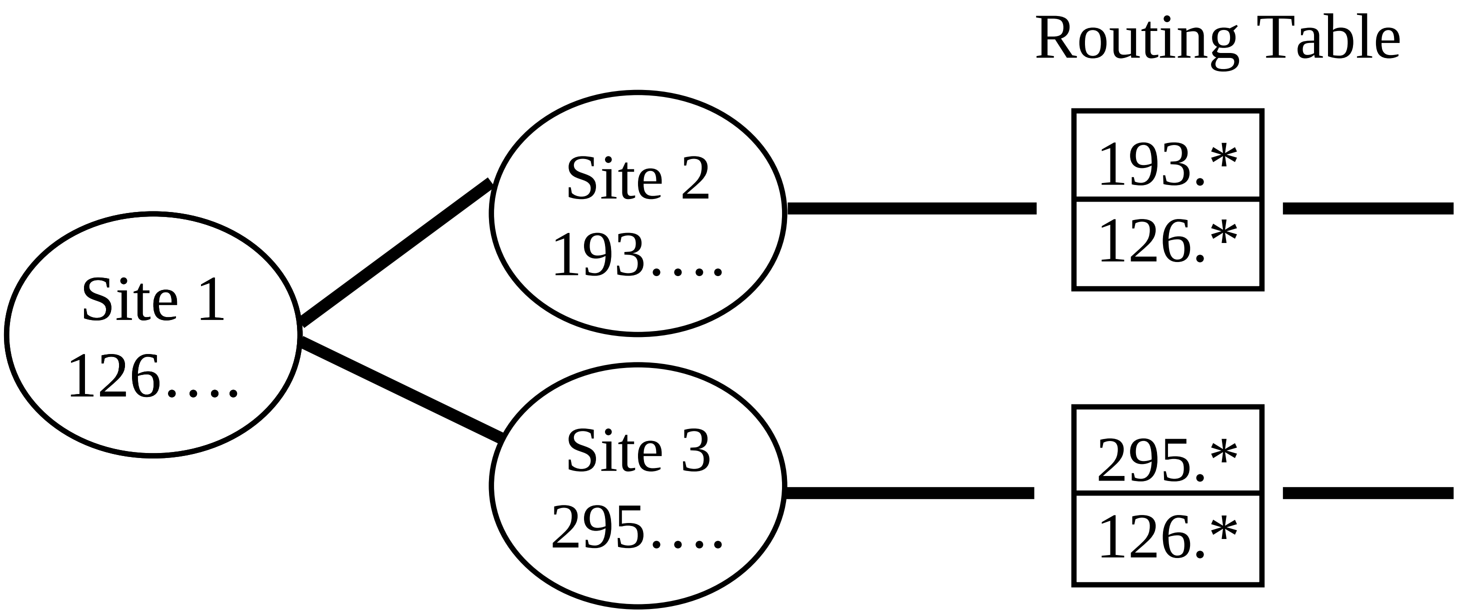
Traffic Engineering

- Multi-homing for load balancing and traffic engineering
- Different paths for different flows
  - Flows = Applications (Voice, Video, Data)
  - Flows = Destination (local, long distance)



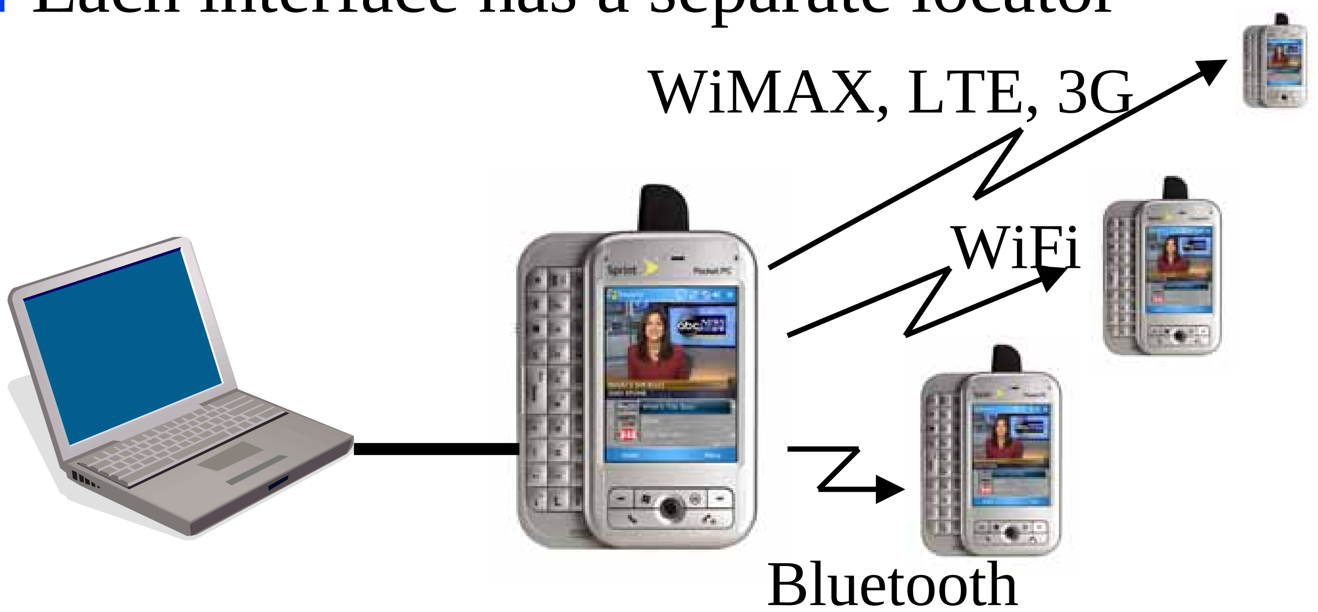
Routing Scalability

- Provider changes ⇒ Change locators for all IP nodes
  ⇒ Provider-Independent (PI) Addresses
  ⇒ Can not be aggregated ⇒ Large routing tables
  ⇒ Scalability



Device Multi-Homing

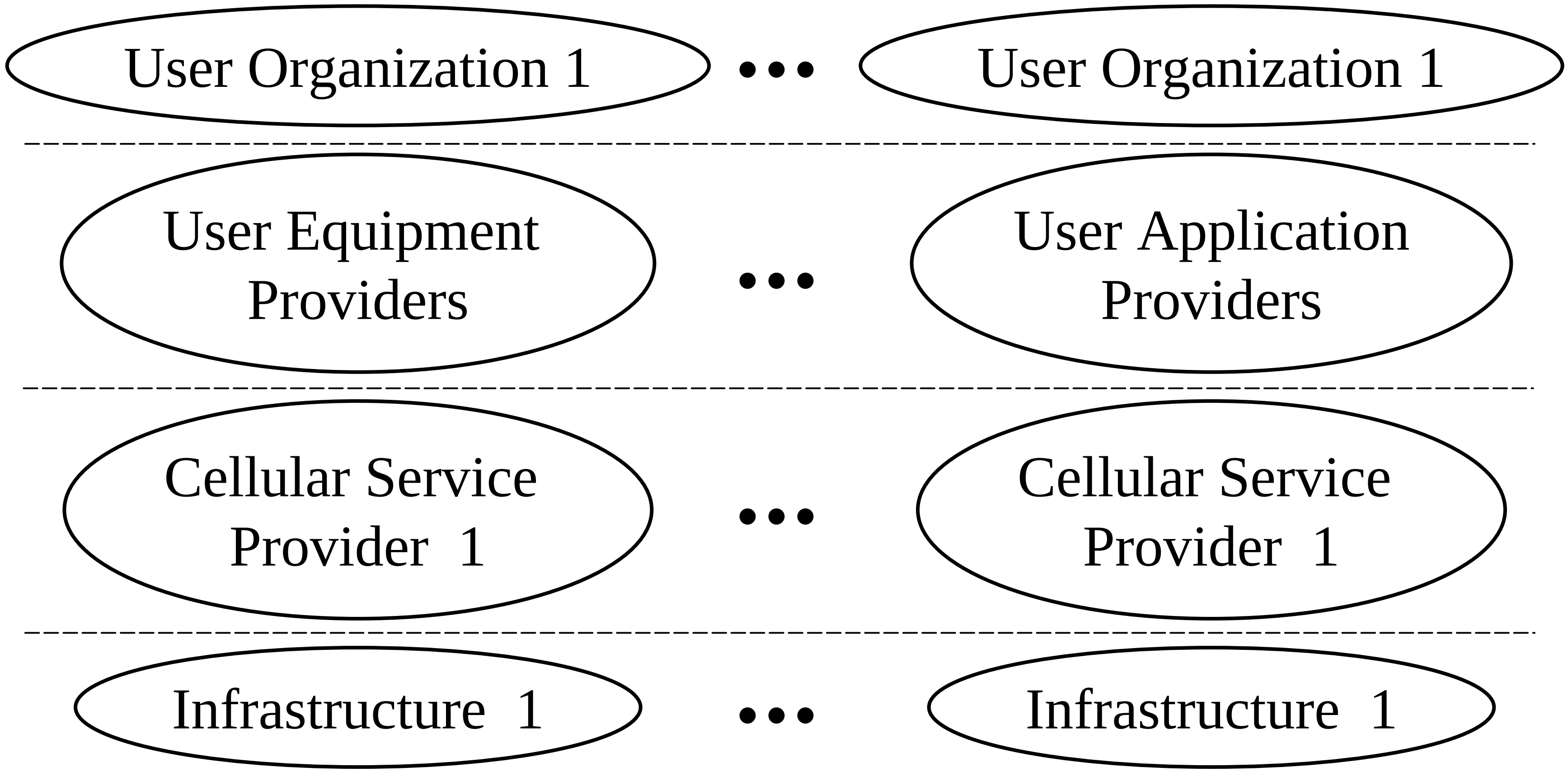
- Each cell phone will have: WiMAX, WiFi, Bluetooth, 3G, and even a wired USB/Ethernet connection for high-speed download/upload
- Each interface has a separate locator



User Multi-Homing

- User multi-homing: Each user will have several cell-phones, desktops, laptops, …
- User ID ⇒ List of Device IDs ⇒ Sets of Locators
- User sets the policies for which devices, interfaces to be used for what type of traffic and correspondents

Multi-Tiered Business Models



- Separate Ownerships: Infrastructure, service, applications, equipment, users => Multi-tiered hierarchy

Organizational Policies

- Location information should be completely in the control of the organization
  - Virtual service providers may not want user organizations to be aware of the infrastructure providers
  - User organizations may not want the locators on one provider to be known to other providers
  - Organizational policies decide which and how many locators can be used for a given application

Impact of ID-Locator Separation

	Feature	Current IP	Post-SAE
1.	Mobility	Slow	Fast
2.		Location privacy with triangulation	Location privacy but no triangulation
3.		Route optimization without location privacy	Route optimization with location privacy
4.	Site Multi-Homing	Requires PI addresses	PI addresses not required. ID's are organization specific.
5.		Causes routing scalability issue	Solves routing scalability issue
6.		Traffic engineering	Provides traffic engineering
7.	Device Multi-Homing	Requires multiple IP addresses TCP cannot move from one interface to another	TCP will be bound to the ID and can easily move among multiple interfaces
8.	User multi-homing	No such concept in current Internet	Users can have ID too.
9.	Ownership	No concept of ownership	Hierarchy of ownerships, administrations, communities
10.	Organizational policies	Organizations are not correctly represented	Organizations can enforce their policies on their users, equipment, and infrastructure

Research Challenges

- Analysis of current ID-Locator separation proposals: LISP, HIP, I3/Hi3, SHIM6, HRA, ...
- Analysis of Mobile IP vs. ID/Locator separation approach

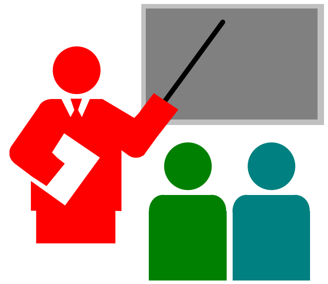
⇒ Survey report on ID/Locator separation approaches

- Develop a new framework for post-SAE ID-Locator separation architecture
  - Methods to better support mobility in post-SAE networks.
  - Methods to better support Multi-homing in post-SAE networks.
  - Methods to better support multi-tiered virtualization helping create virtual service providers over shared infrastructure

Migration Challenges

- Lessons from the technologies of the past, e.g., IPv6, Mobile IP vs. NAT, Carrier Ethernet, …
- Need to develop a smooth migration strategy
- Low cost (firmware upgrades vs. new hardware)
- Must co-exist with the existing legacy infrastructure
- Incremental changes should provide immediate benefits $\Rightarrow$ One site updating to new Post-SAE should benefit while the other sites are still using legacy
- The benefits increase as more and more sites adopt the new architecture

Summary of Part I

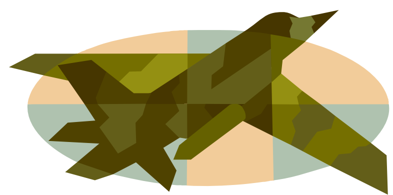


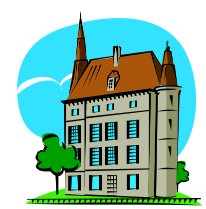
1. In the current Internet architecture, IP address is used both as an ID as well as a locator
2. ID-Locator separation will help fix: Mobility, Multi-homing, Traffic Engineering, Routing Scalability
3. Need to emphasize device and user multi-homing (along with site multi-homing)
4. Multi-tiered Virtualization is required to support future cellular networks
5. Organizational policies for security, privacy, and authentication need to be considered in ID-locator separation

Our Proposed Solution: Internet 3.0

- Internet 3.0 is the name of the Washington University project on the next generation Internet Protocol architecture
- Named by me along the lines of "Web 2.0"
- Inspired by US National Science Foundation's research and infrastructure program on next generation Internet
  - Testbed: "Global Environment for Networking Innovations" (GENI)
  - Architecture: "Future Internet Design" (FIND).
- Takes the best of what is already known

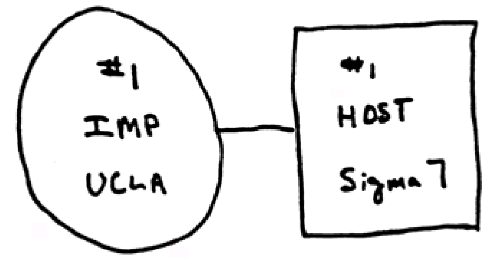


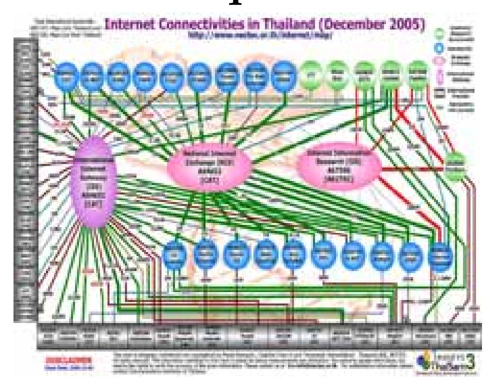


Internet Generations

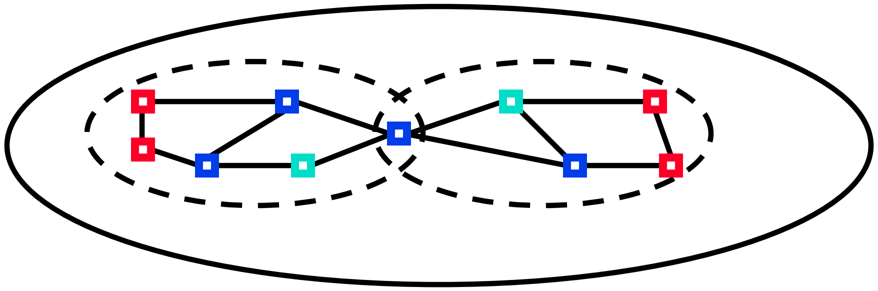
- **Internet 1.0** (1969 – 1989) – Research project
  - RFC1 is dated April 1969.
  - ARPA project started a few years earlier
  - IP, TCP, UDP
  - Mostly researchers
  - Industry was busy with proprietary protocols: SNA, DECnet, AppleTalk, XNS



- **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,…



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

Physical vs. Logical Connectivity

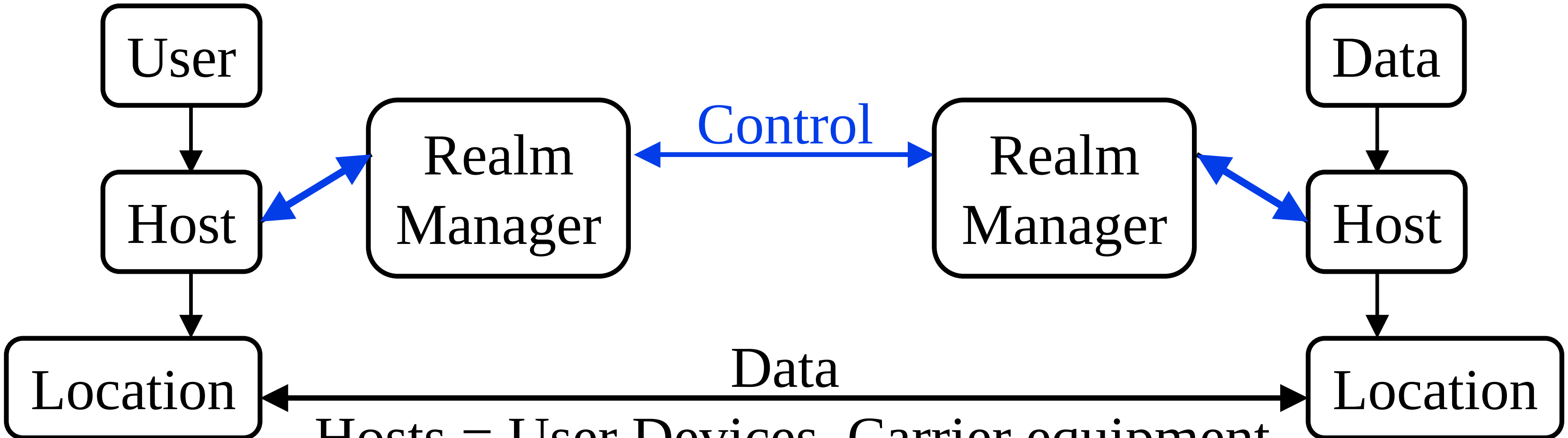
- Physically and logically connected:
  All computers in my lab
  = Private Network,
  Firewalled Network

- 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

Id-Locator Split Architecture (MILSA)



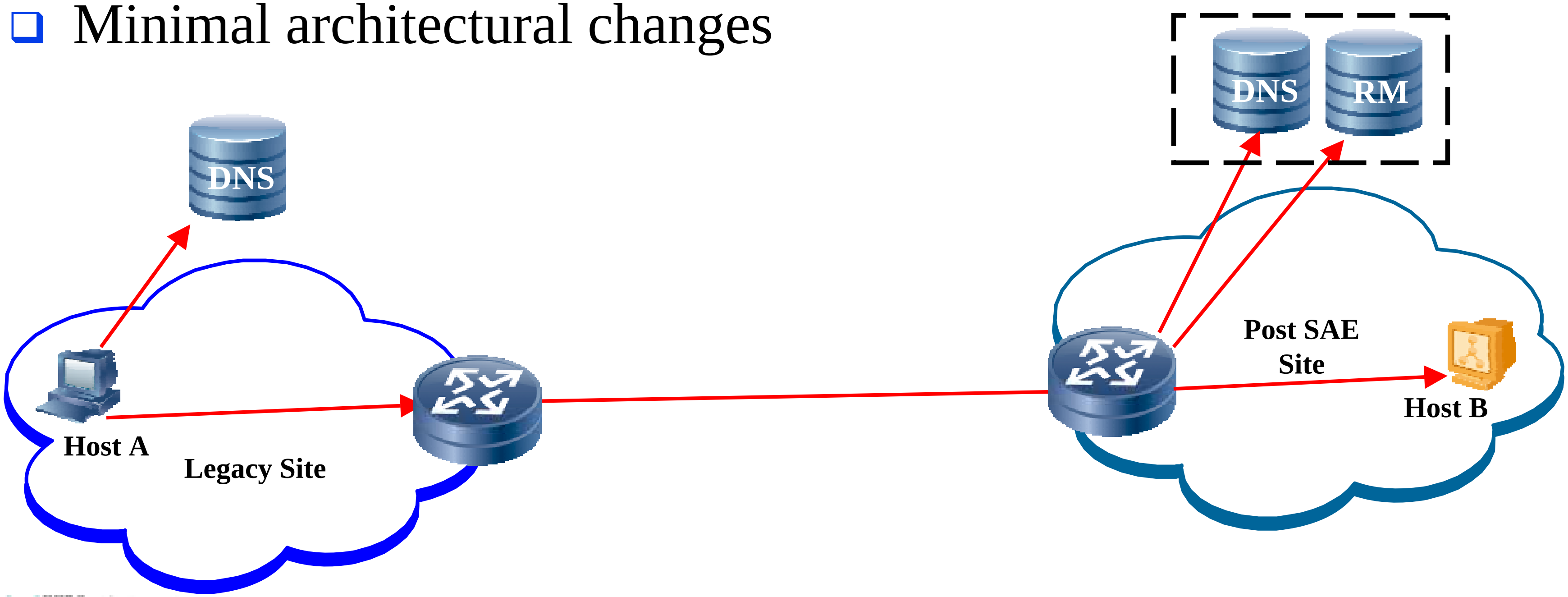
Hosts = User Devices, Carrier equipment

Realm managers:

- Resolve current location for a given host-ID
- Enforce policies related to authentication, authorization, privacy
- Allow mobility, multi-homing, location privacy
- Different from several other ID-locator splitting proposals. Our Emphasis on organizational control.
- Ref: Our Globecom 2008 paper [2]

Internet 3.0 Naming Architecture: MILSA

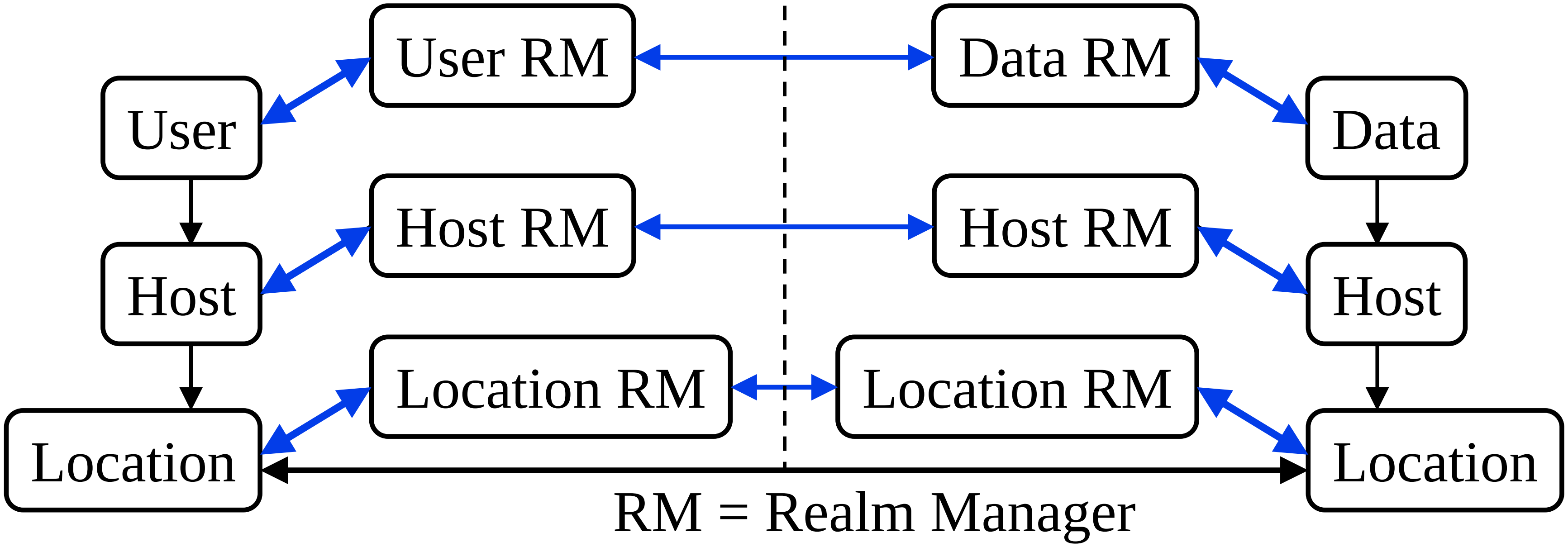
- **M**ulti-homing supporting **I**dentifier **L**ocator **S**plit **A**rchitecture
- Realm Manager (RM) function is similar to Domain Name System (DNS) can can be implemented as an upgrade to DNS but RM is owned by the organization
- Minimal architectural changes



User- Host- and Data Centric Models

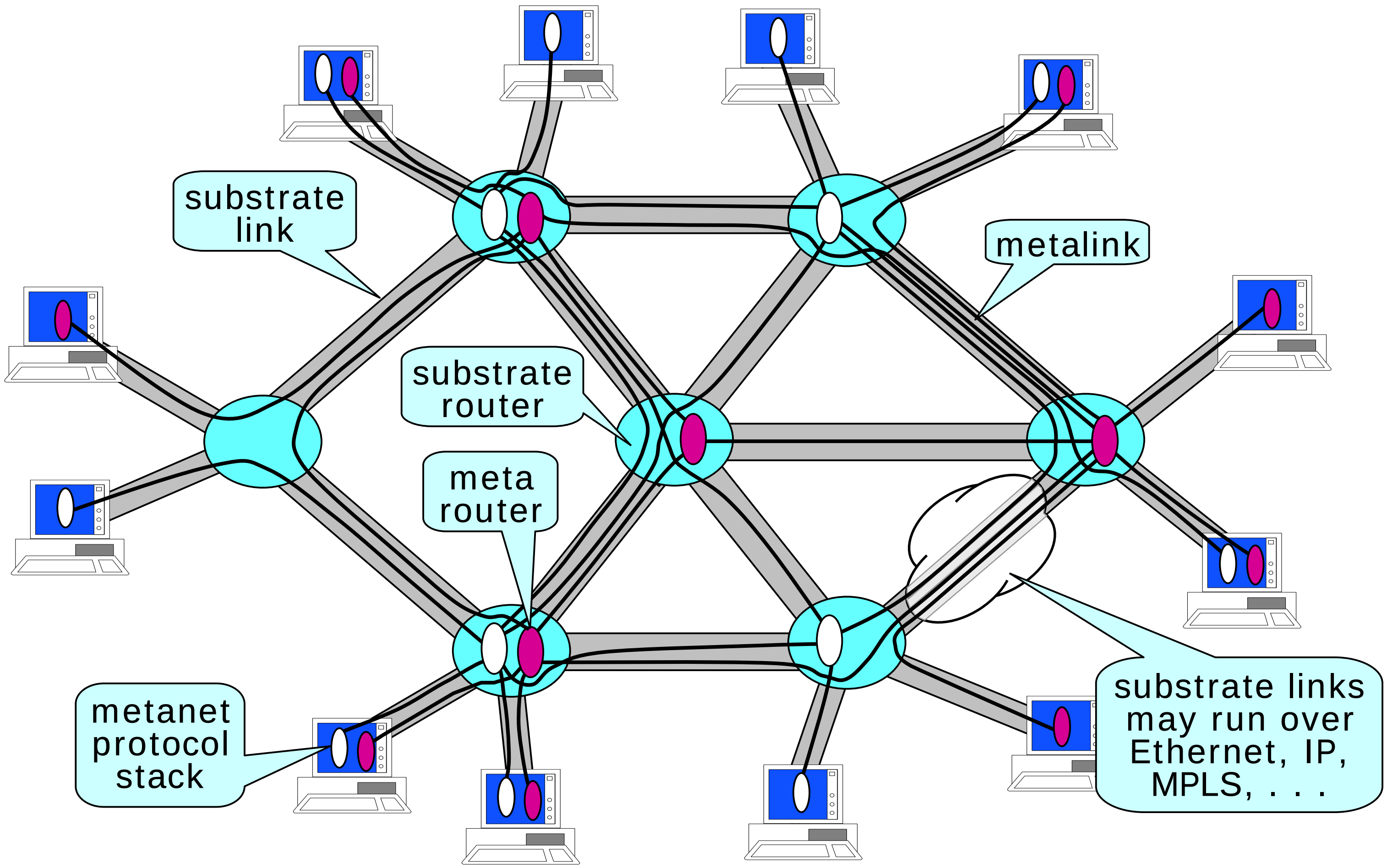
- All discussion so far assumed host-centric communication
  - Host mobility and multihoming
  - Policies, services, and trust are related to hosts
- User Centric View:
  - Bob wants to watch a movie
  - Starts it on his media server
  - Continues on his iPhone during commute to work
  - Movie exists on many servers
  - Bob may get it from different servers at different times or multiple servers at the same time
- Can we just give addresses to users and treat them as hosts? No! ⇒ Policy Oriented Naming Architecture (PONA)

Policy Oriented Naming Architecture



- Both Users and data need hosts for communication
- Data is easily replicable. All copies are equally good.
- Users, Hosts, Infrastructure, Data belong to different realms (organizations).
- Each object has to follow its organizational policies.

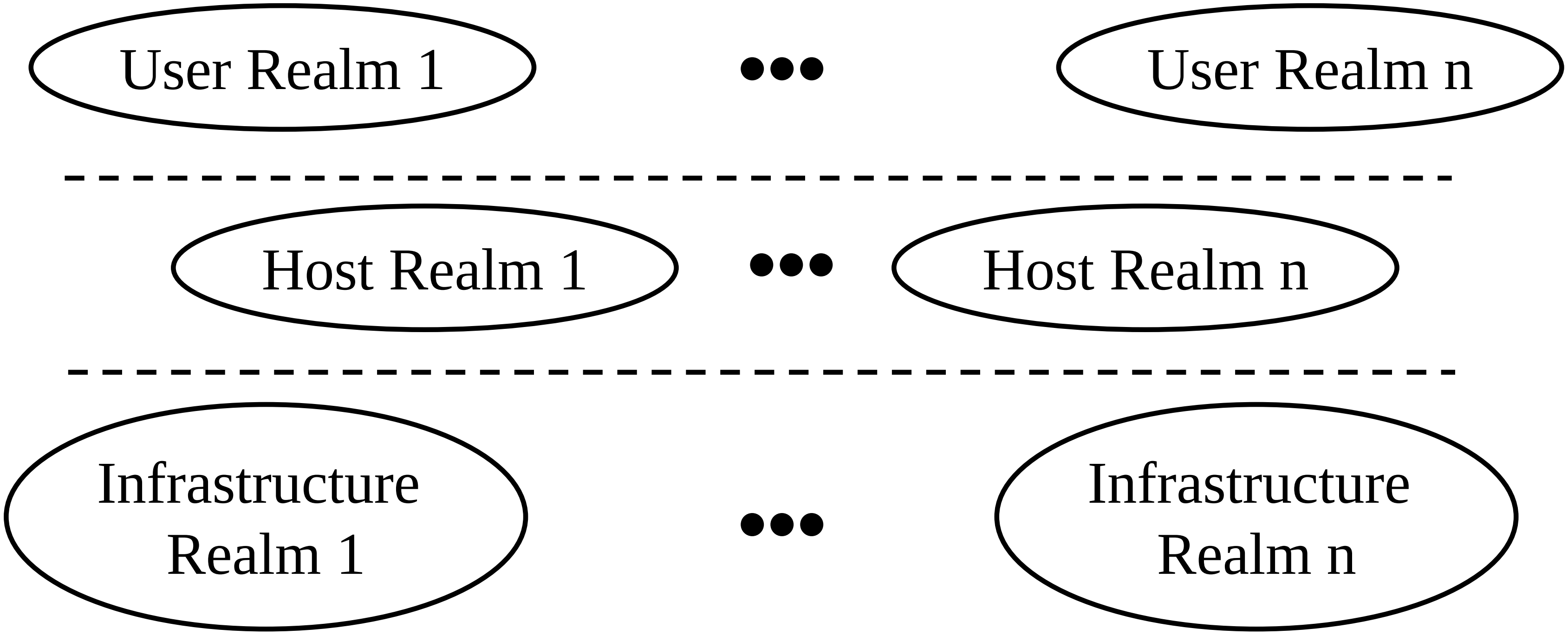
Virtualizable Network Concept



Ref: T. Anderson, L. Peterson, S. Shenker, J. Turner, "Overcoming the Internet Impasse through Virtualization," Computer, April 2005, pp. 34 – 41.

Slide taken from Jon Turner's presentation at Cisco Routing Research Symposium

Realm Virtualization

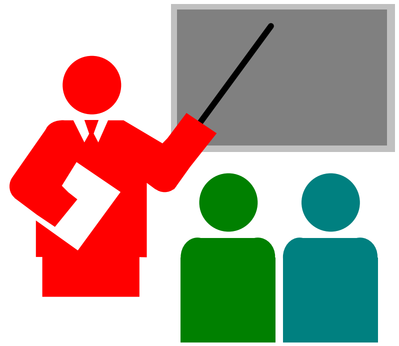


- Old: Virtual networks on a common infrastructure
- New: Virtual user realms on virtual host realms on a group of infrastructure realms. 3-level hierarchy not 2-level. Multiple organizations at each level.

Internet 1.0 vs. Internet 3.0

	Feature	Internet 1.0	Internet 3.0
1.	Energy Efficiency	Always-on	Green ⇒ Mostly Off
2.	Mobility	Mostly stationary computers	Mostly mobile *objects*
3.	Computer-Human Relationship	Multi-user systems ⇒ Machine to machine comm.	Multi-systems user ⇒ Personal comm. systems
4.	End Systems	Single computers	Globally distributed systems
5.	Protocol Symmetry	Communication between equals ⇒ Symmetric	Unequal: PDA vs. big server ⇒ Asymmetric
6.	Design Goal	Research ⇒ Trusted Systems	Commerce ⇒ No Trust Map to organizational structure
7.	Ownership	No concept of ownership	Hierarchy of ownerships, administrations, communities
8.	Sharing	Sharing ⇒ Interference, QoS Issues	Sharing *and* Isolation ⇒ Critical infrastructure
9.	Switching units	Packets	Packets, Circuits, Wavelengths, Electrical Power Lines, …
10.	Applications	Email and Telnet	Information Retrieval, Distributed Computing, Distributed Storage, Data diffusion

Summary of Part II



1. Internet 3.0 is the next generation of Internet.
2. It must be secure, allow mobility, and be energy efficient.
3. Must be designed for commerce
   ⇒ Must represent multi-organizational structure and policies
4. Moving from host centric view to user-data centric view
   ⇒ Important to represent users and data objects
5. Users, Hosts, and infrastructures belong to different realms (organizations). Users/data/hosts should be able to move freely without interrupting a network connection.

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)

4. Jianli Pan, Raj Jain, Subharthi Paul, Mic Bowman, Xiaohu Xu, Shanzhi Chen, "Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet," To appear in Proceedings of IEEE International Conference in Communications (ICC) 2009, Dresden, Germany, June 14-18, 2009, (sponsored by Huawei) http://www.cse.wustl.edu/~jain/papers/emilsa.htm

谢谢 Thank You!


Hvala
Grazie
धन्यवाद
Bedankt
Teşekkürler
Díky
Köszönettel
ขอบคุณ
شكراً
Ευχαριστώ
Merci
Gracias
Obrigado!
Vielen Dank
תודה