ITU-T Workshop on Addressing security challenges on a global scale

6 – 7 December 2010 Geneva, Switzerland

Security Aspects of Locator/ID Separation Protocol

Gregg Schudel

Cisco Systems, Inc.

gschudel@cisco.com

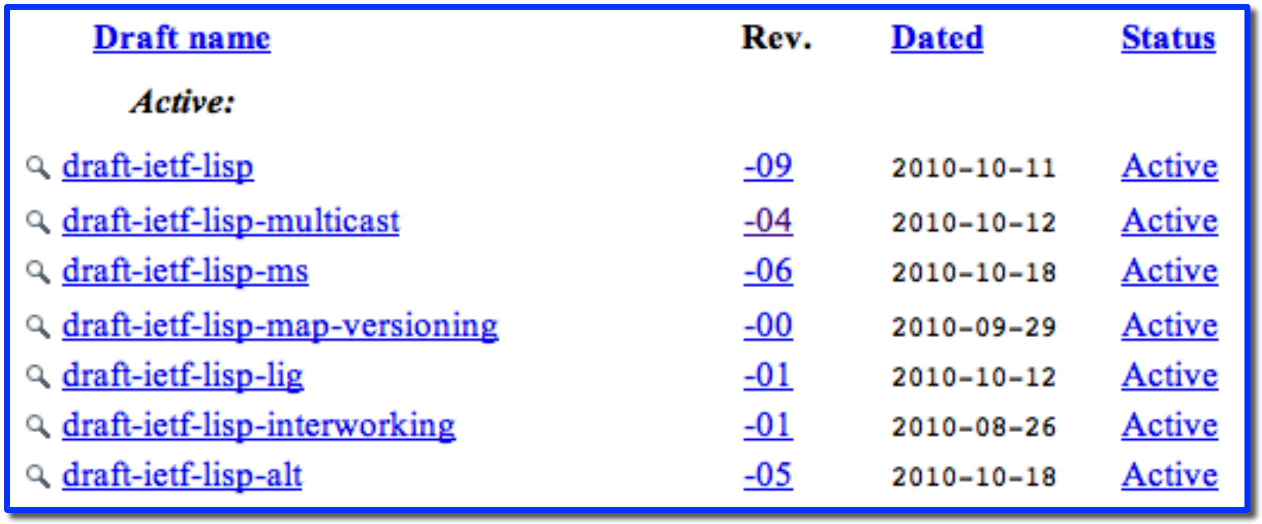
Agenda

1. LISP Overview
2. LISP Benefits
3. Security Aspects of LISP
4. Questions?
5. References

LISP Overview

LISP is the “Locator/ID Separation Protocol”

LISP is being developed under the IETF LISP WG

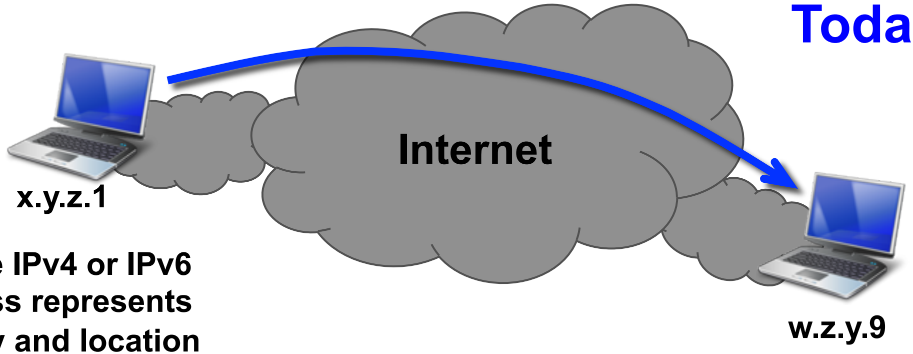


Draft name	Rev.	Dated	Status
Active:			
draft-ietf-lisp	-09	2010-10-11	Active
draft-ietf-lisp-multicast	-04	2010-10-12	Active
draft-ietf-lisp-ms	-06	2010-10-18	Active
draft-ietf-lisp-map-versioning	-00	2010-09-29	Active
draft-ietf-lisp-lig	-01	2010-10-12	Active
draft-ietf-lisp-interworking	-01	2010-08-26	Active
draft-ietf-lisp-alt	-05	2010-10-18	Active

Similarly named ITU-T efforts (e.g. SG13) are not the same as the IETF version of LISP

LISP Overview

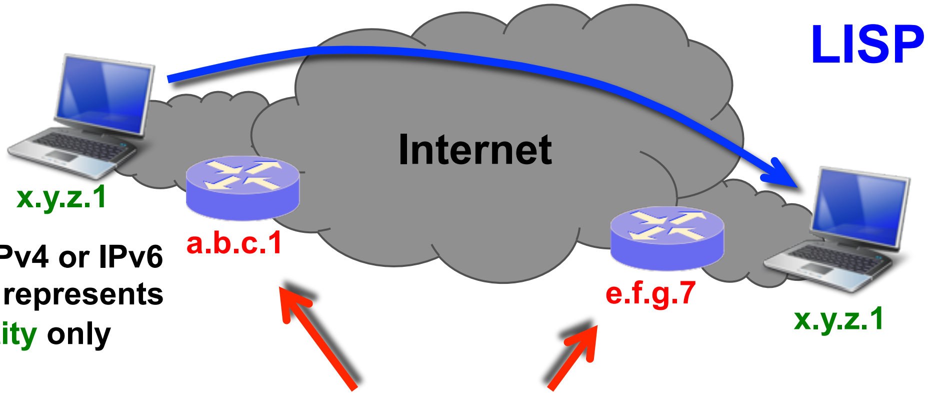
Today's Internet Behavior



Device IPv4 or IPv6
address represents
identity and location

When the device moves, it gets
a new IPv4 or IPv6 address for
its new identity and location

LISP Behavior



Device IPv4 or IPv6
address represents
identity only

When the device moves, keeps
its IPv4 or IPv6 address.
It has the same identity

Only the location changes

LISP Overview

IP encapsulation scheme

- Decouples host IDENTITY and LOCATION
- Dynamic IDENTITY-to-LOCATION mapping resolution
- Address Family agnostic day-one

  IPv4-in-IPv4, IPv4-in-IPv6, IPv6-in-IPv4, IPv6-in-IPv6

Minimal Deployment Impact

- No changes to end systems or core
- Minimal changes to edge devices

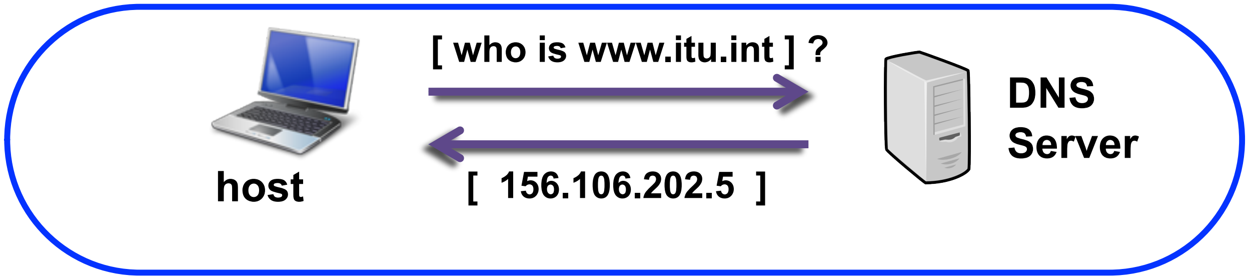
Incrementally deployable

- LISP-to-LISP and LISP-to-non-LISP considered day-one

LISP Overview

LISP Map Lookup is analogous to a DNS lookup

- DNS resolves IP addresses for URLs



host

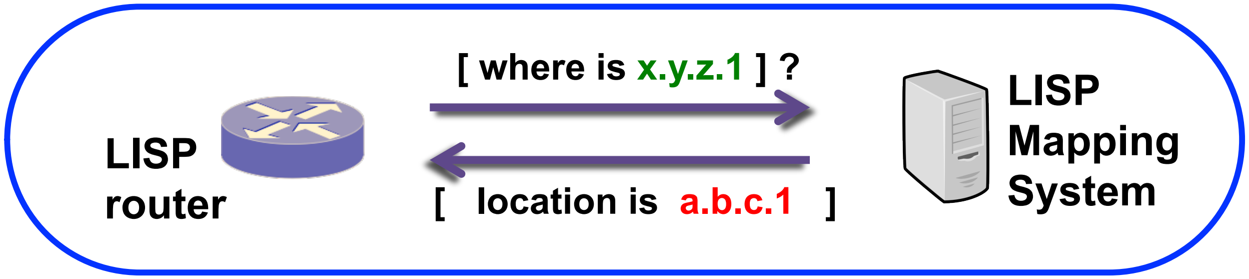
[who is www.itu.int] ?

[156.106.202.5]

DNS
Server

DNS
URL Resolution

- LISP resolves locators for queried identities



LISP
router

[where is x.y.z.1] ?

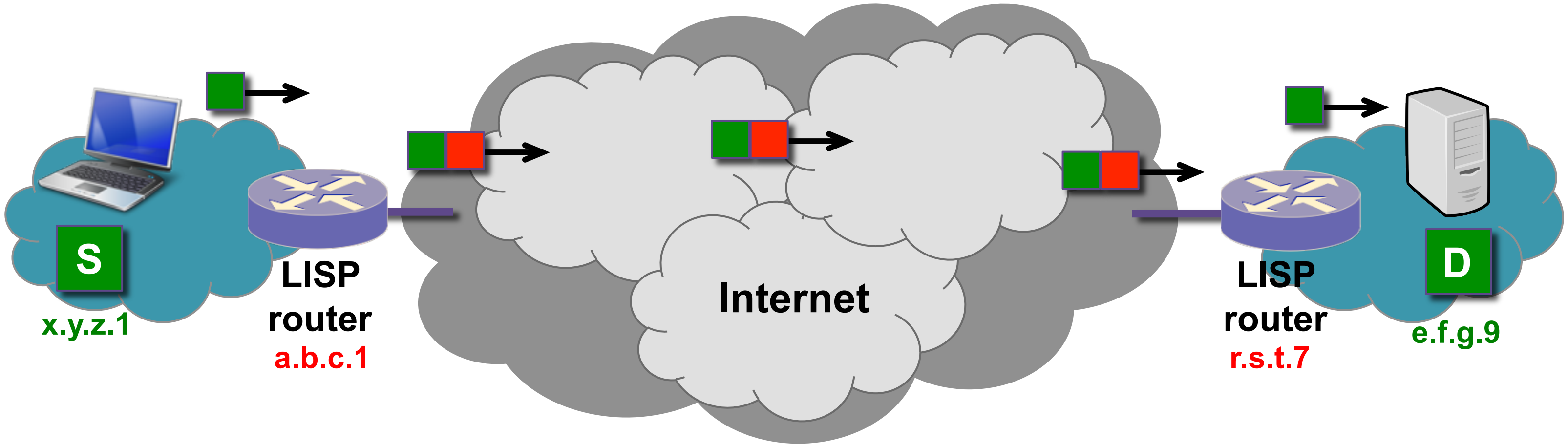
[location is a.b.c.1]

LISP
Mapping
System

LISP
Identity-to-location
Map Resolution

LISP Overview

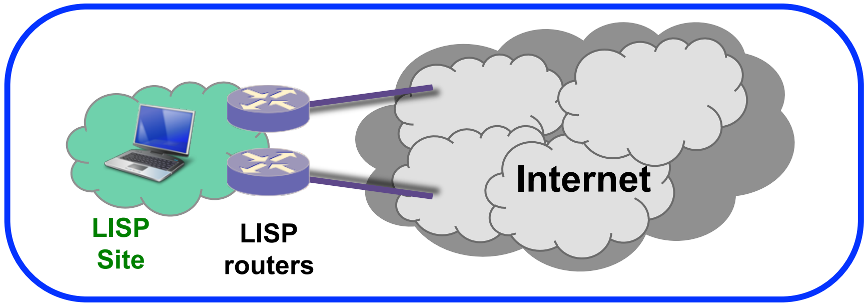
LISP Forwarding



LISP Overview

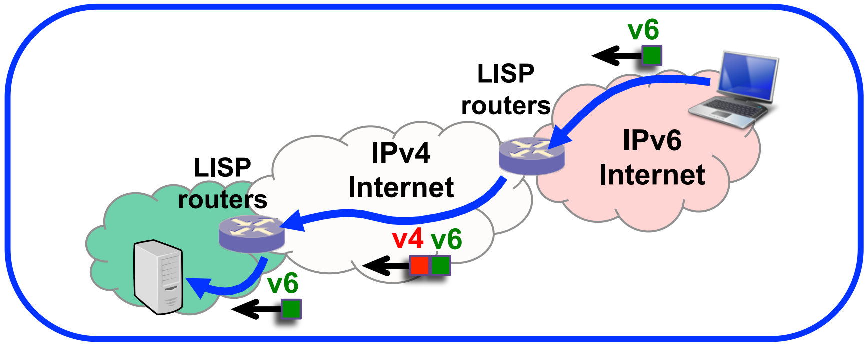
Efficient Multi-Homing

- IP Portability
- Ingress Traffic Engineering without BGP



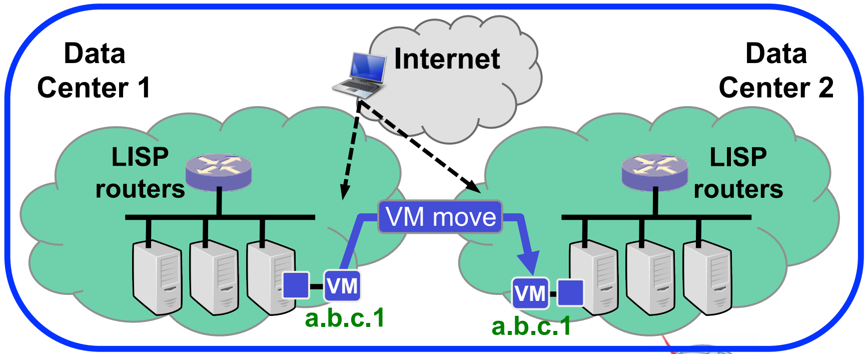
IPv6 Transition Support

- v6-over-v4
- v4-over-v6



VM-Mobility

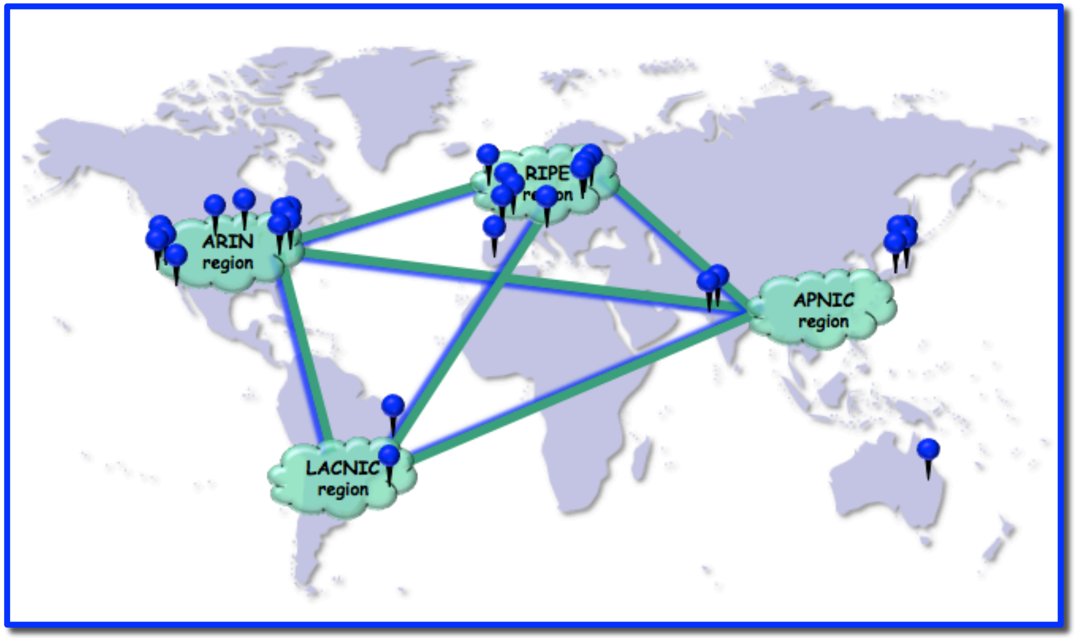
- Cloud Computing
- Segmentation



LISP Overview

LISP is deployed!

- >3 years
- >85 sites
- 13 countries



Six Implementations

- Cisco: IOS, NX-OS
- FreeBSD: OpenLISP
- Linux: two (2) implementations
- Android

No Intellectual Property – open design

Security Aspects of LISP

Security…

… of the protocol

- Inherent security of the protocol itself

… impact of the protocol on existing network security

- Changes that can be/need be made to a site and core network to handle the protocol

… enabled by the protocol

- New types of network security that can be deployed because of the new protocol

Security Aspects of LISP

Security… of the protocol

Internet + LISP is no less secure than existing Internet

- The protocol must be "deployable"

Security of the protocol is added as driven by operational requirements

- Authentication of Map-Registers
- Nonce in Map-Request/Map-Reply
- Other internal specifications (see Internet draft)

Protocol developed to be enhanced by other security mechanisms as needed: e.g.

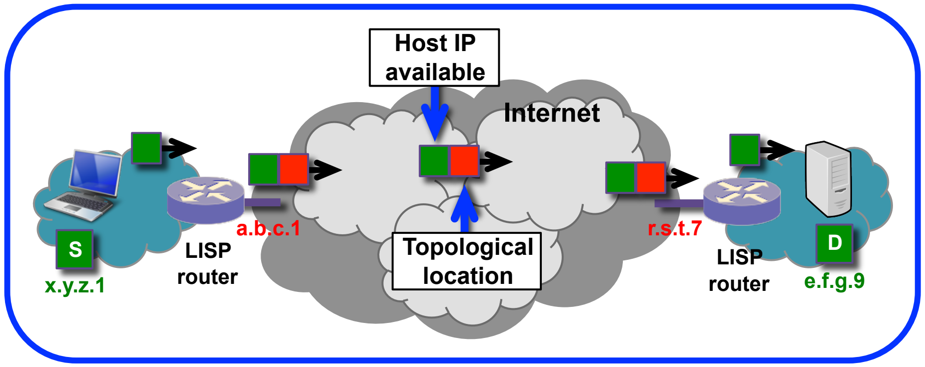
- IPsec and Group Encrypted Transport (GET)
- PKI for control plane

Security Aspects of LISP

Security… impact of protocol on existing network security

Core/Internet Point of Reference

- Inner (host) address still available to core for policy enforcement
  - Requires recognition of LISP encapsulation
  - No different than GRE, MPLS, or other encapsulations



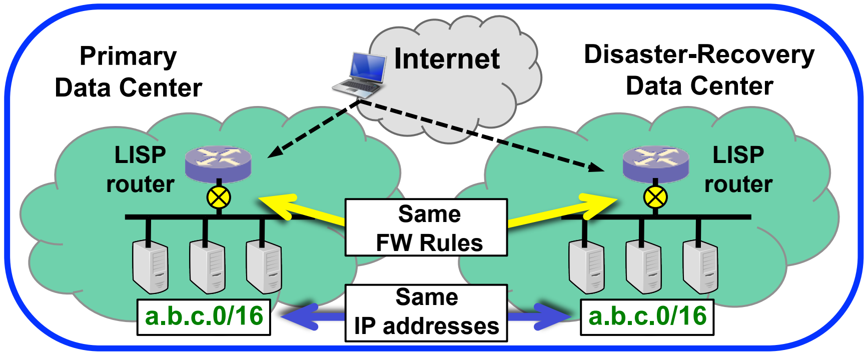
  - This is much better than NAT which obscures original IP address
- Outer address points to “topological” location

Security Aspects of LISP

Security… impact of protocol on existing network security

Site Point of Reference

- No changes to existing Firewall and ACL policies since the original packets are still visible
- Simplified access-control policy development and enforcement



Security Aspects of LISP

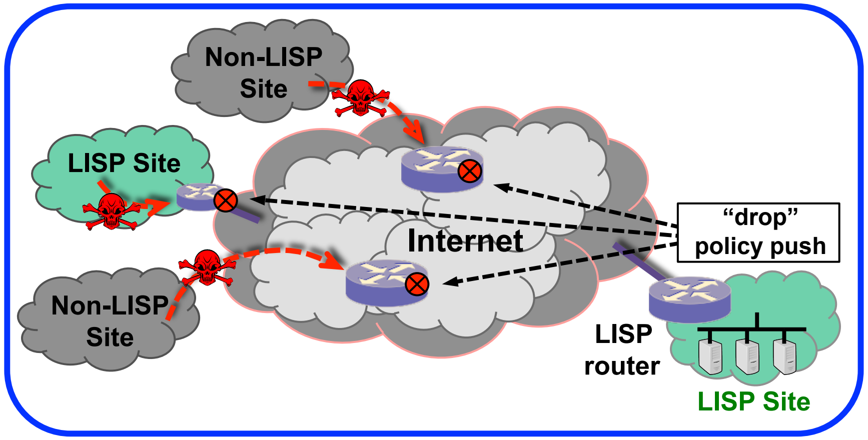
Security… enabled by the protocol

Simplified Firewall and ACL policies

- Host IP address (identity) never changes
  - policy enforcement by “identity” not by “location”

New Mechanisms from “built-in” LISP functions

- Ingress traffic engineering mechanism can be used as a DDoS “push-back” policy
  - Push a “drop” policy all the way back to the encapsulator
  - Simple “redirection” to scrubber center

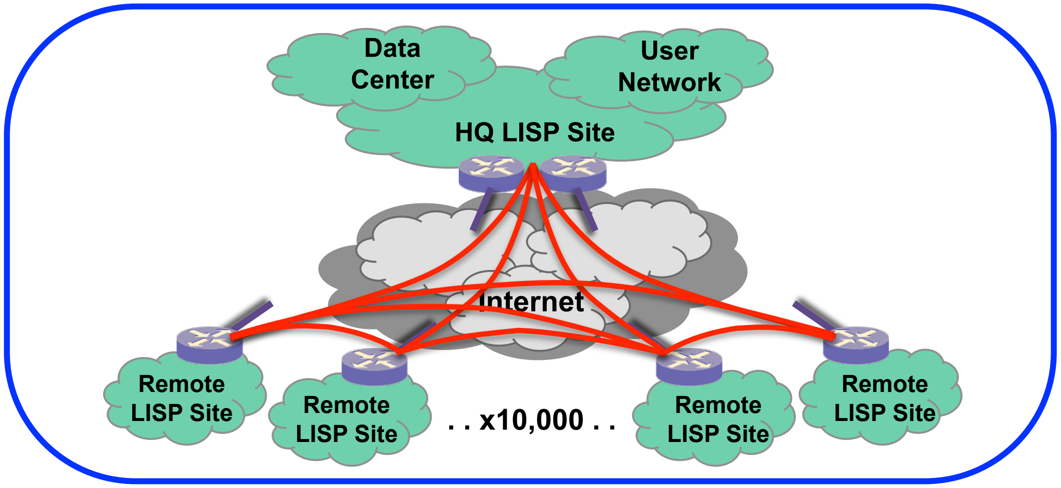


Security Aspects of LISP

Security… enabled by the protocol

New Mechanisms from "built-in" LISP functions (cont.)

- Enables ability to deploy "high-scale VPNs" of >10,000 sites
  - Routing protocol (and other state) typically limit the scale of VPNs
  - Out-of-band LISP control-plane enables high-scale VPNs



Questions?

References

LISP Information

- IETF LISP WG http://tools.ietf.org/wg/lisp/
- LISP Beta Network http://www.lisp4.net http://www.lisp6.net
- Cisco LISP Site http://lisp4.cisco.com http://lisp6.cisco.com

Mailing Lists

- IETF LISP WG lisp@ietf.org
- LISP Interest lisp-interest@puck.nether.net