LISP - A Next Generation Routing Architecture

Cisco Mid-Atlantic Users Group
September 13, 2011

Craig Hill
Distinguished Systems Engineer
Cisco Systems, Inc.

LISP Use Case Examples

About the Speaker

- **Craig Hill**

- Worked at Cisco Systems from 1995 – Present (16 years), CCIE #1628
- Focus past 11 years has been on Service Provider technologies and architectures, specifically in DoD and the IC
- Technical focus areas: IP/MPLS, network virtualization (specific focus over IP/MPLS), HA and convergence, Carrier Ethernet, QoS, IPv6, Integration of IP/MPLS + optical/DWDM, and network focus for DC, video, and Cloud Compute networks. And… LISP ☺
- Other internal roles includes: technology evangelist positioning and architecture integration into business relevant customer solutions, field rep for product development in routing, Technical Lead – Advanced Routing Team (Federal)
- Cisco Live Presenter : 2009 – 2011, WAN Virtualization Concepts and design, Enterprise Network Virtualization
- Contact info: Email: crhill@cisco.com, Twitter: @netwrkr95
- More Content? Google “craig hill cisco systems”

LISP Use Case - Agenda

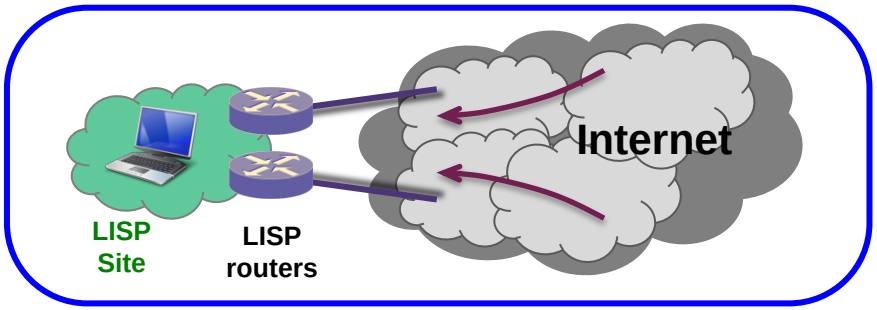
- LISP Use Cases
- LISP Standards Update
- Summary
- HW/SW Roadmap
- References

LISP Use Cases
The Five Core LISP Use-Cases

1. Efficient Multi-Homing
2. IPv6 Transition Support
3. Network Virtualization/Multi-Tenancy
4. Data Center/VM Mobility
5. LISP Mobile-Node

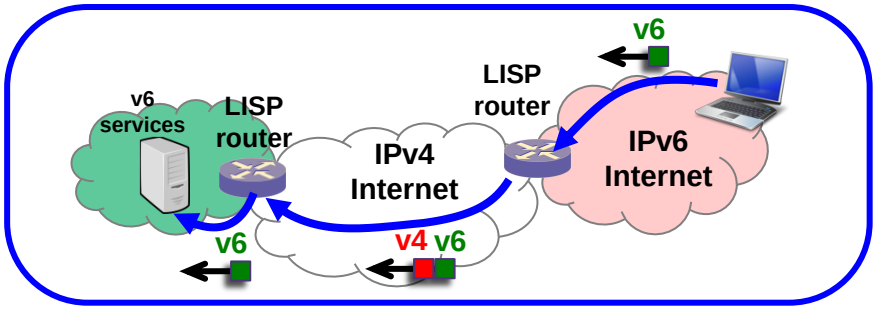
LISP Use Cases
Overview

Efficient Multi-Homing



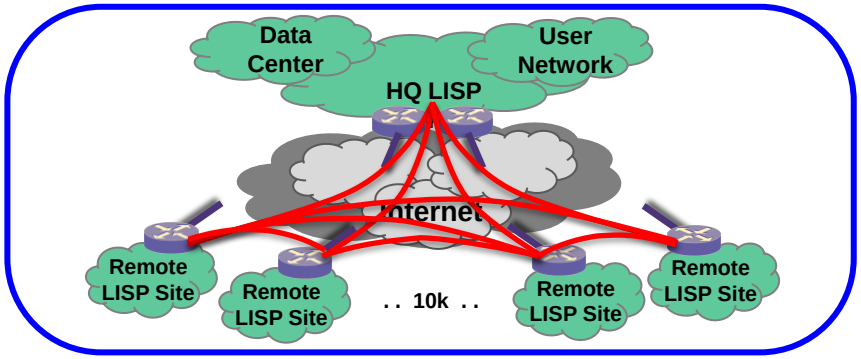
- IP Portability
- Ingress Traffic Engineering without BGP

IPv6 Transition Support



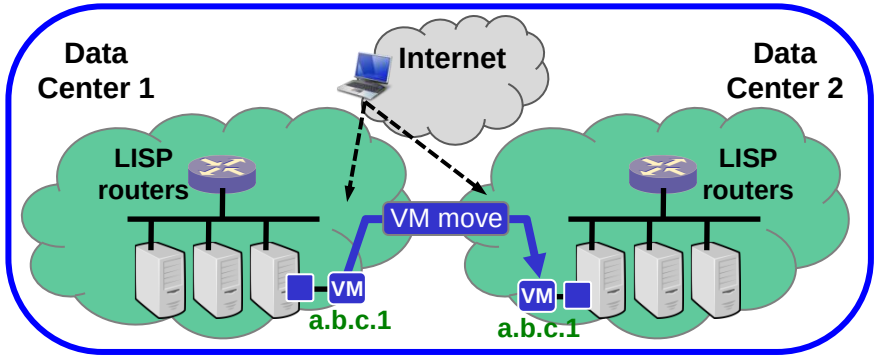
- v6-over-v4, v6-over-v6
- v4-over-v6, v4-over-v4

Network Virtualization - VPN



- Reduced CapEx/OpEx
- Segmentation

VM-Mobility



- Cloud / Layer 3 VM moves
- Segmentation

LISP Use Cases
Efficient Multi-Homing

Needs:

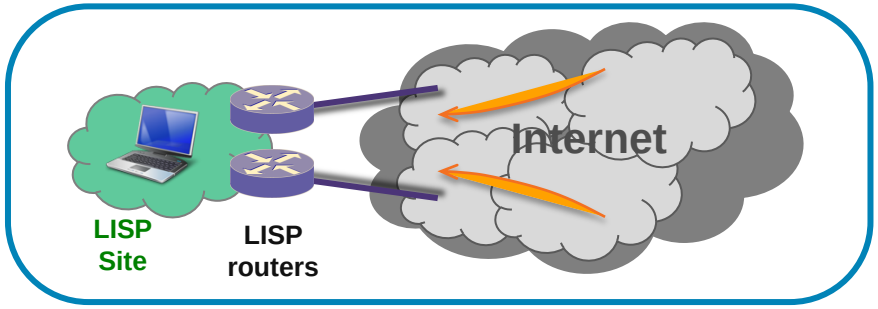
- Site connectivity to multiple providers
- Low OpEx/CapEx

LISP Solution:

- LISP provides a streamlined solution for handling multi-provider connectivity and policy without BGP complexity

Benefits:

- Multi-homing across different providers
- Simple policy management
- Ingress Traffic Engineering
- Egress Traffic Engineering



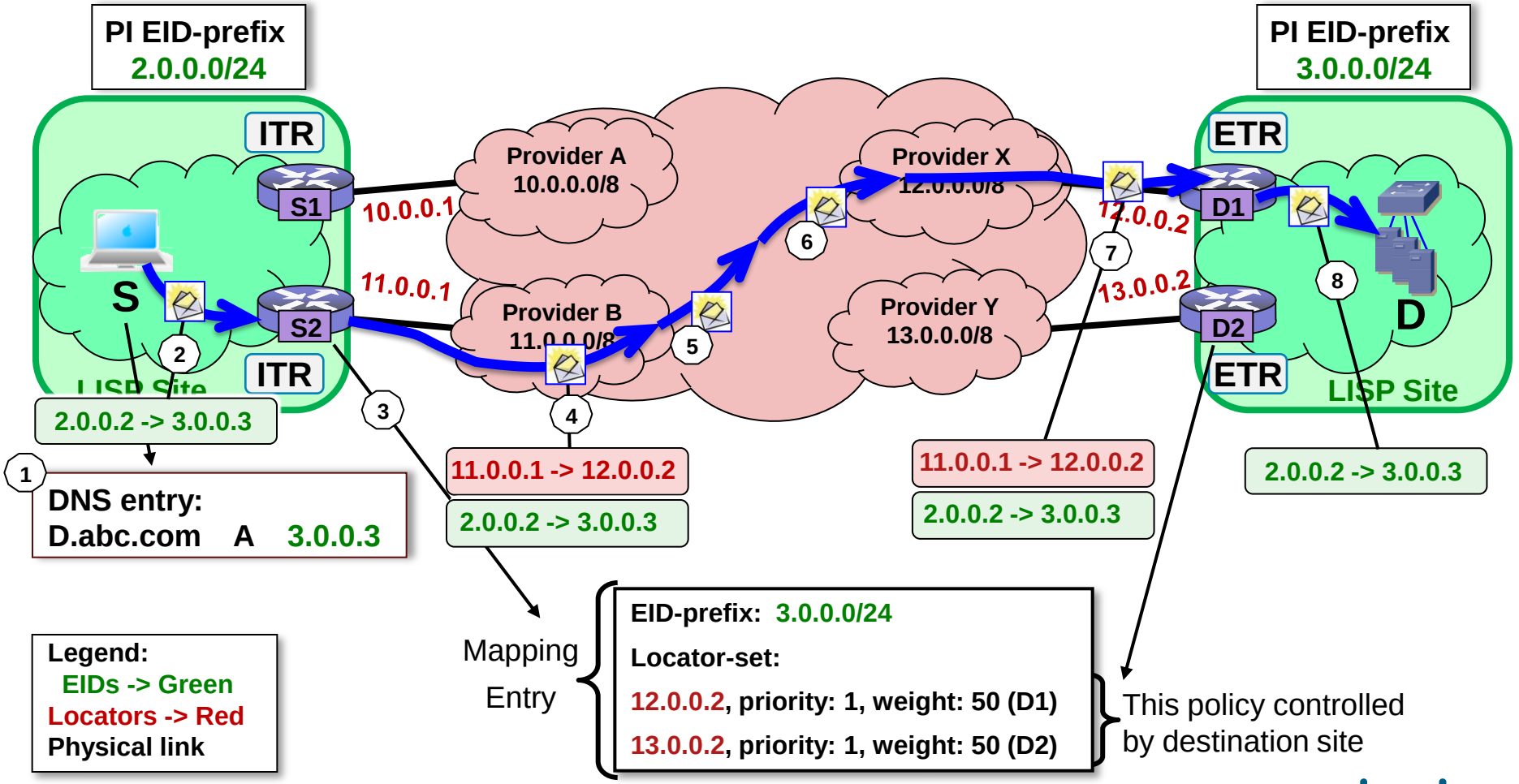
Applicability:

- Branch sites where multihoming is traditionally too expensive
- Useful in all other LISP Use Cases

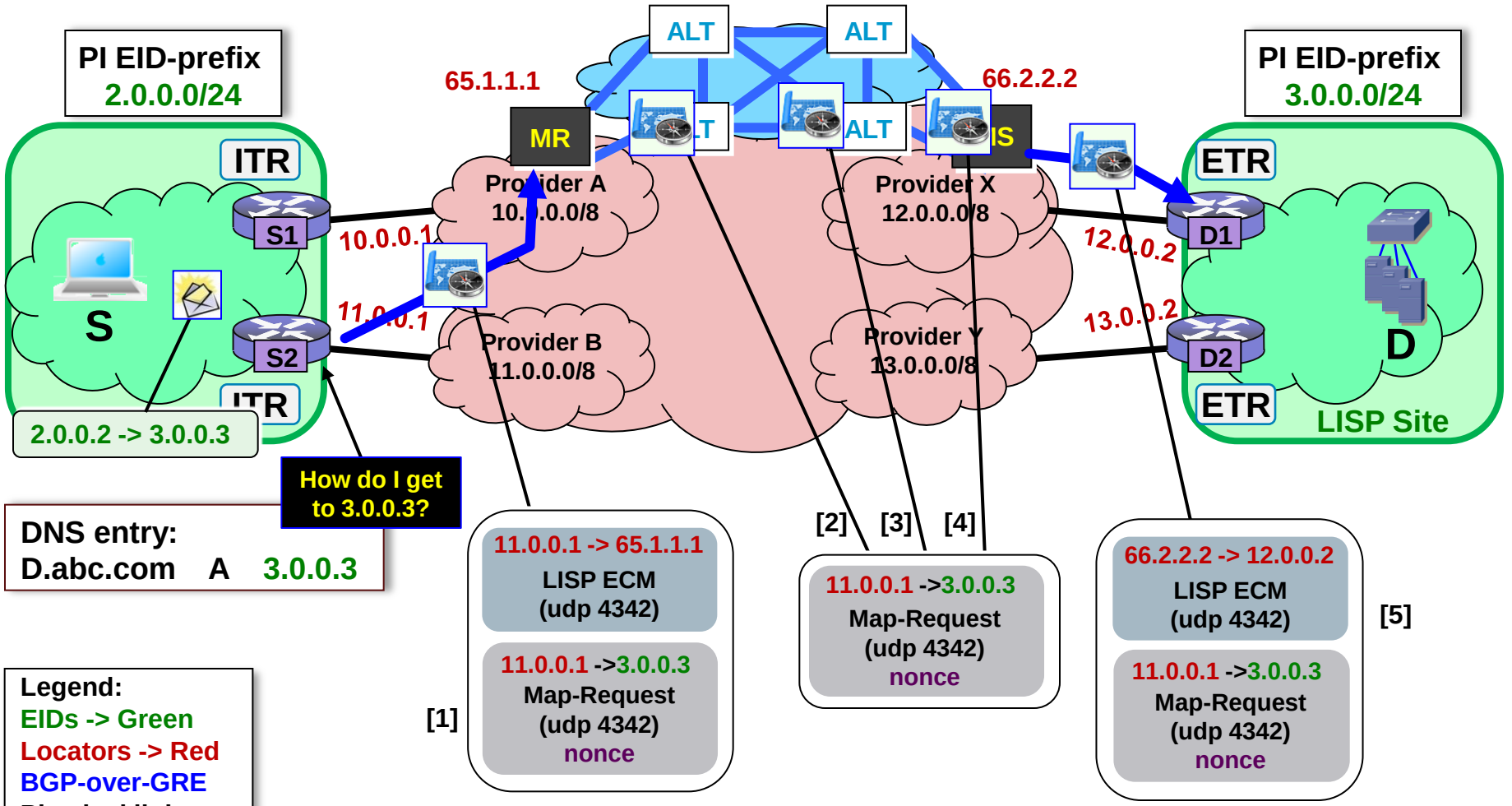
Customers/EFTs:

- Qualcomm
- Verizon Business
- Cisco IT

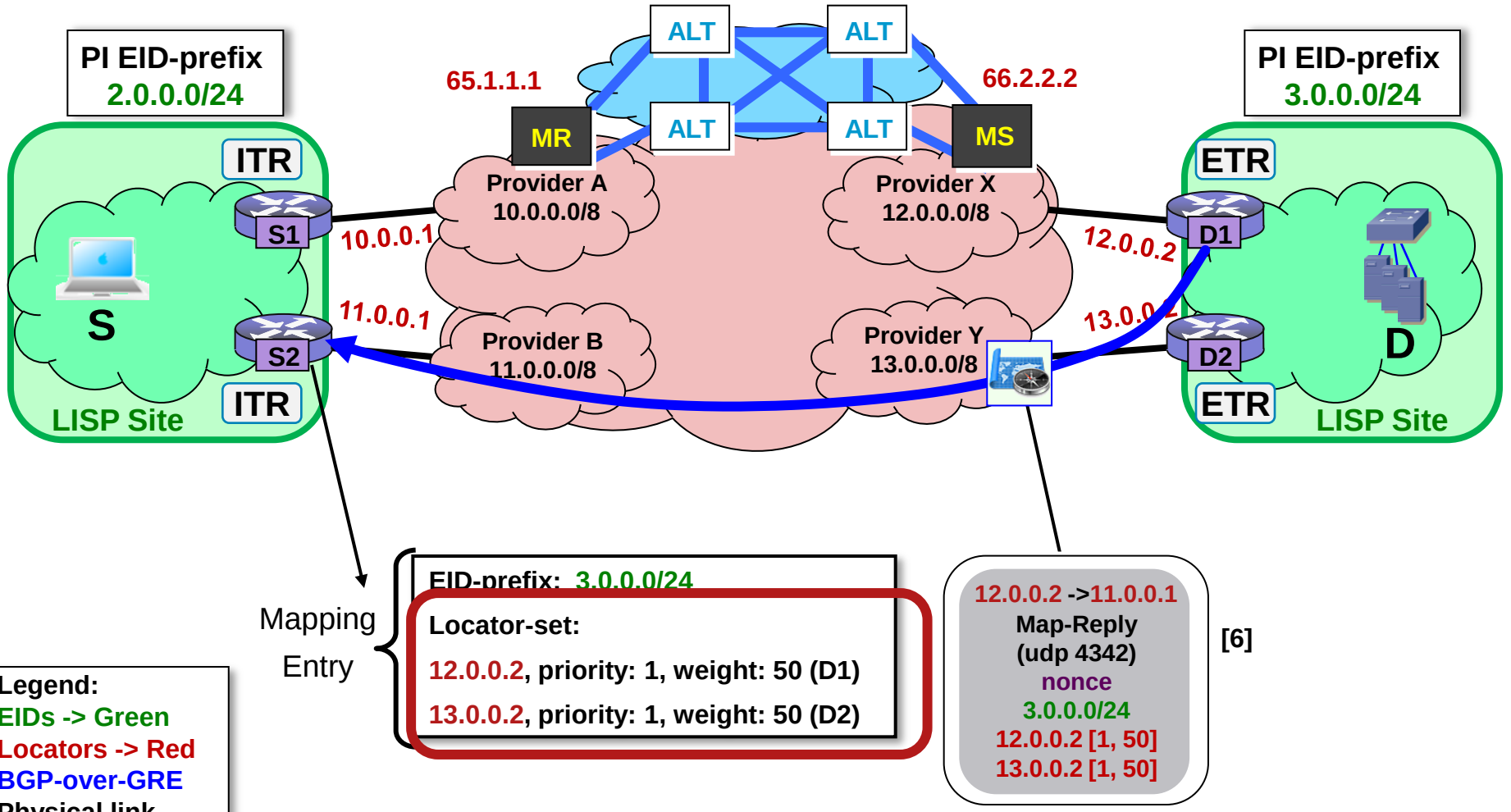
LISP Use Cases
Efficient Multi-Homing – Unicast Forwarding Review



LISP Use Cases
Efficient Multi-Homing – Control Plane - Review



LISP Use Cases
Efficient Multi-Homing – Control Plane - Review



‘database-mapping’ Command

database-mapping

To configure an IPv4 or IPv6 EID-to-RLOC mapping relationship and its associated traffic policy use the **database-mapping command in LISP configuration mode.**

Syntax Description

EID-prefix/prefixlength

The IPv4 or IPv6 EID prefix and length to be advertised by this router.

locator

The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix/prefix-length

priority *priority* *The priority (value between 0 and 255) assigned to the RLOC. When multiple locators* have the same priority they may be used in load-shared fashion. A lower value indicates a higher priority.

weight *weight* *The weight (value between 0 and 100) assigned to the locator, used to determine how to* load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.configured with only its own locators.

database-mapping 172.16.91.0/24 10.1.1.1 priority 1 weight 50
database-mapping 172.16.91.0/24 10.2.1.1 priority 1 weight 50

LISP Use Cases
IPv6 Transition Support

Needs:

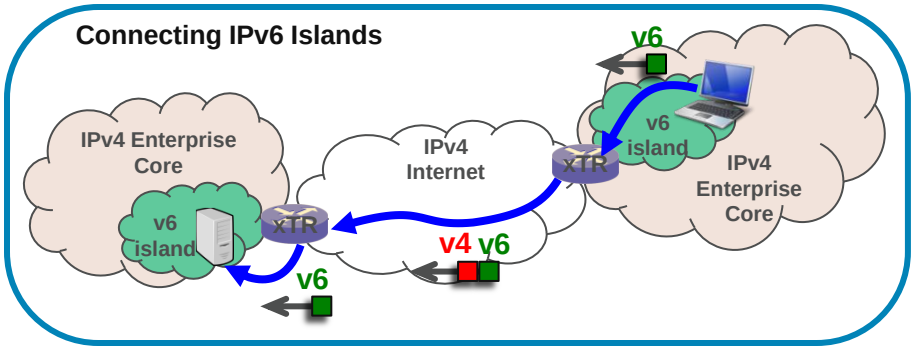
- Rapid IPv6 Deployment
- Minimal Infrastructure disruption

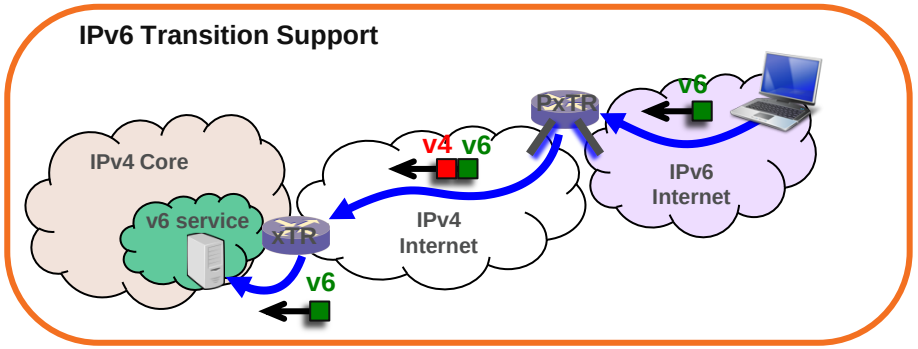
LISP Solution:

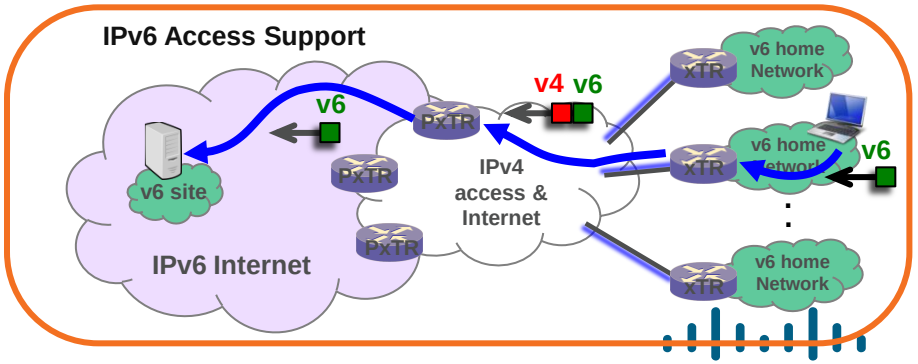
- LISP encapsulation is Address Family agnostic
  - IPv6 interconnected over IPv4 core
  - IPv4 interconnected over IPv6 core

Benefits:

- Accelerated IPv6 adoption
- Minimal added configurations
- No core network changes
- Can be used as a transitional or permanent solution

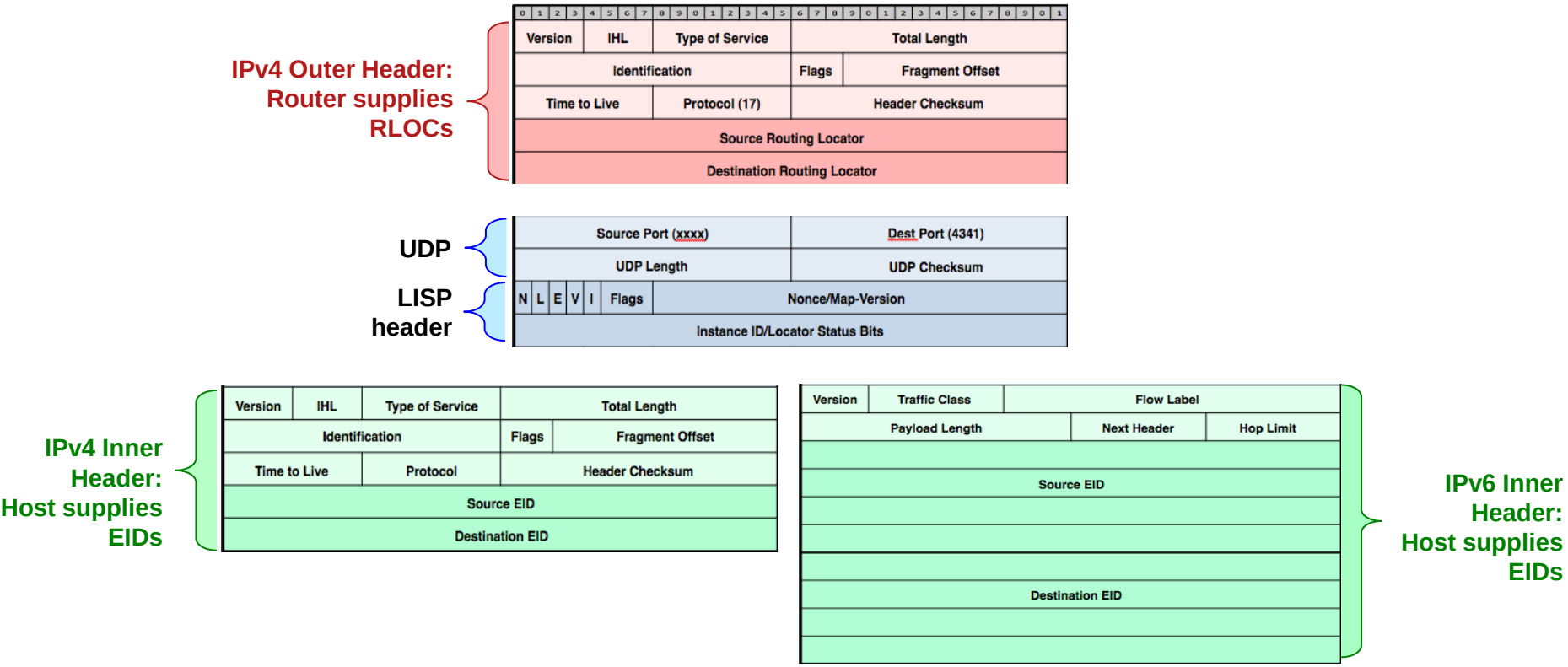






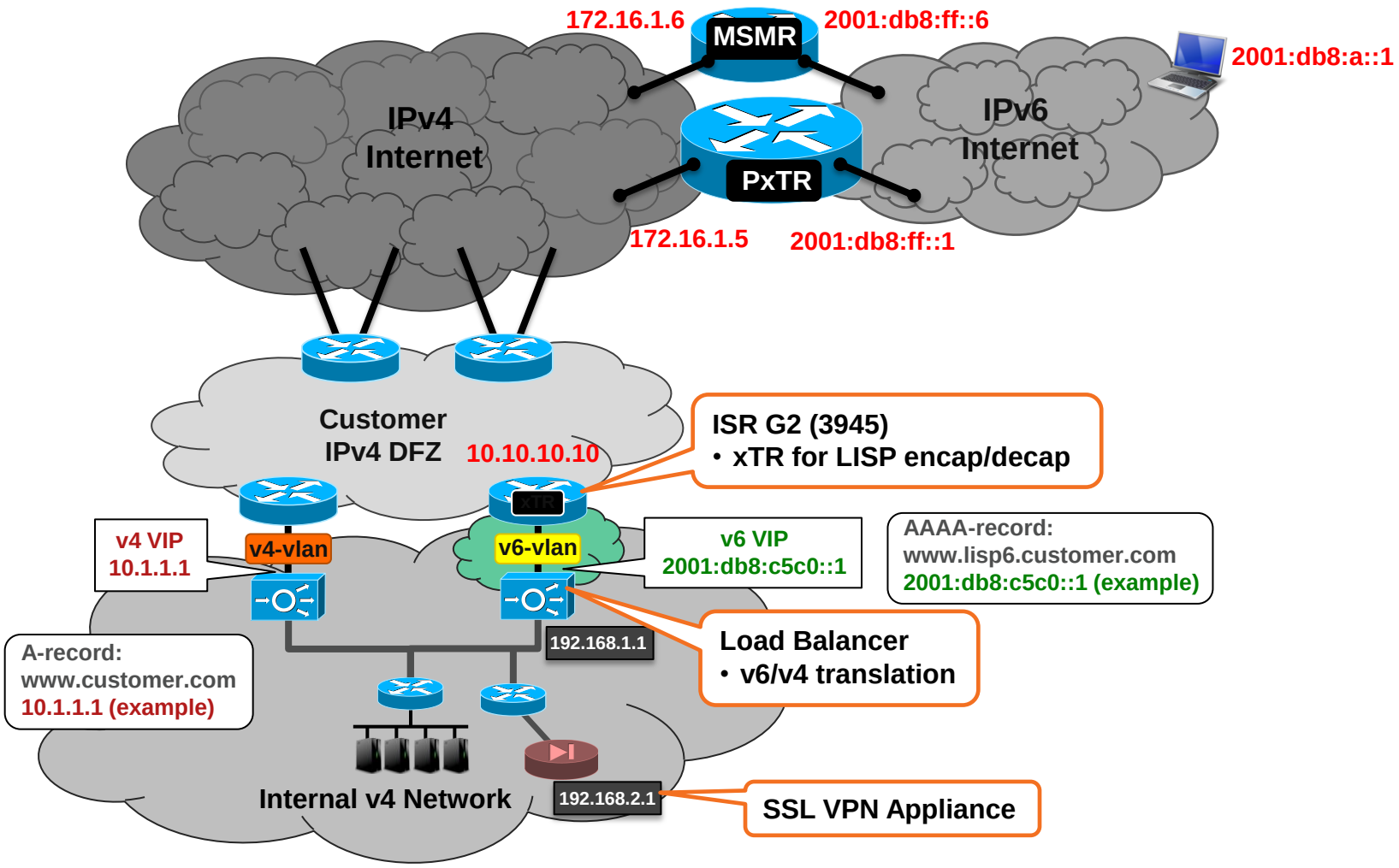
LISP – Data Header Format

IPv4 RLOC with IPv4 EID or IPv6 EID

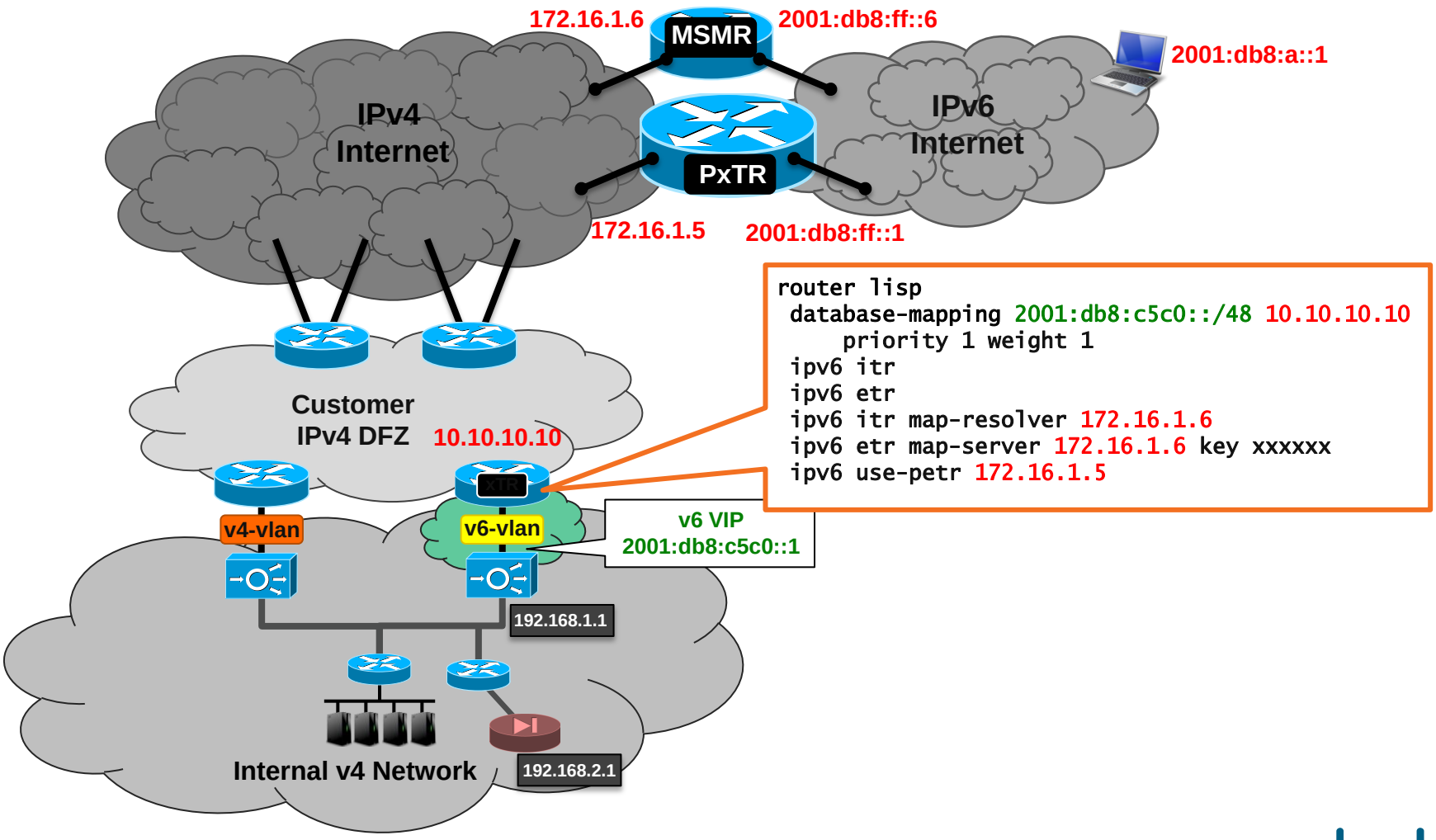


- Outer Header could be IPv6 also
- UDP En-Cap to better load-split the encapsulated packets across member links of such LAGs
- Otherwise, core routers would see a single flow

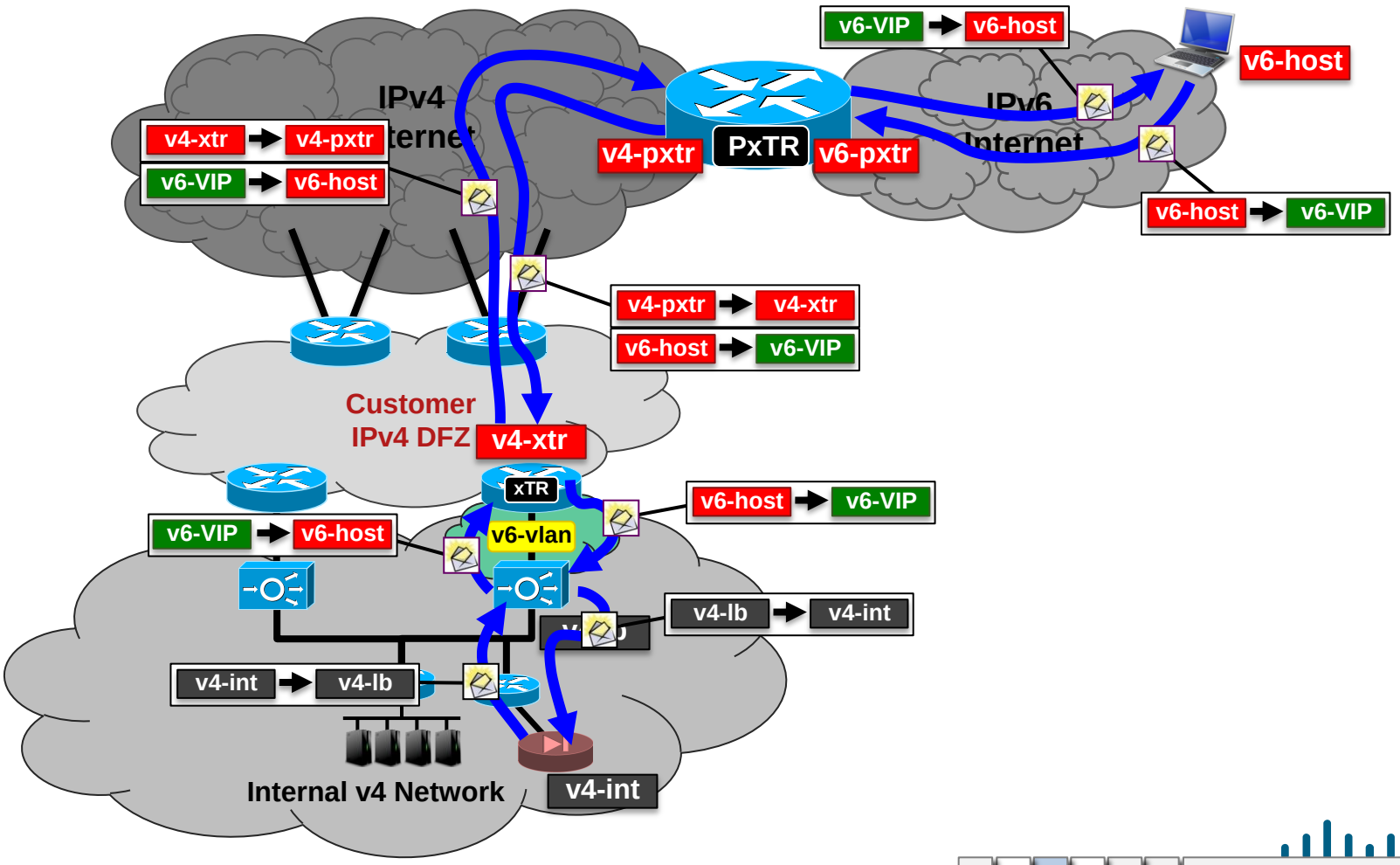
LISP Use Cases – IPv6 Migration Support
Customer Case Study – General Topology



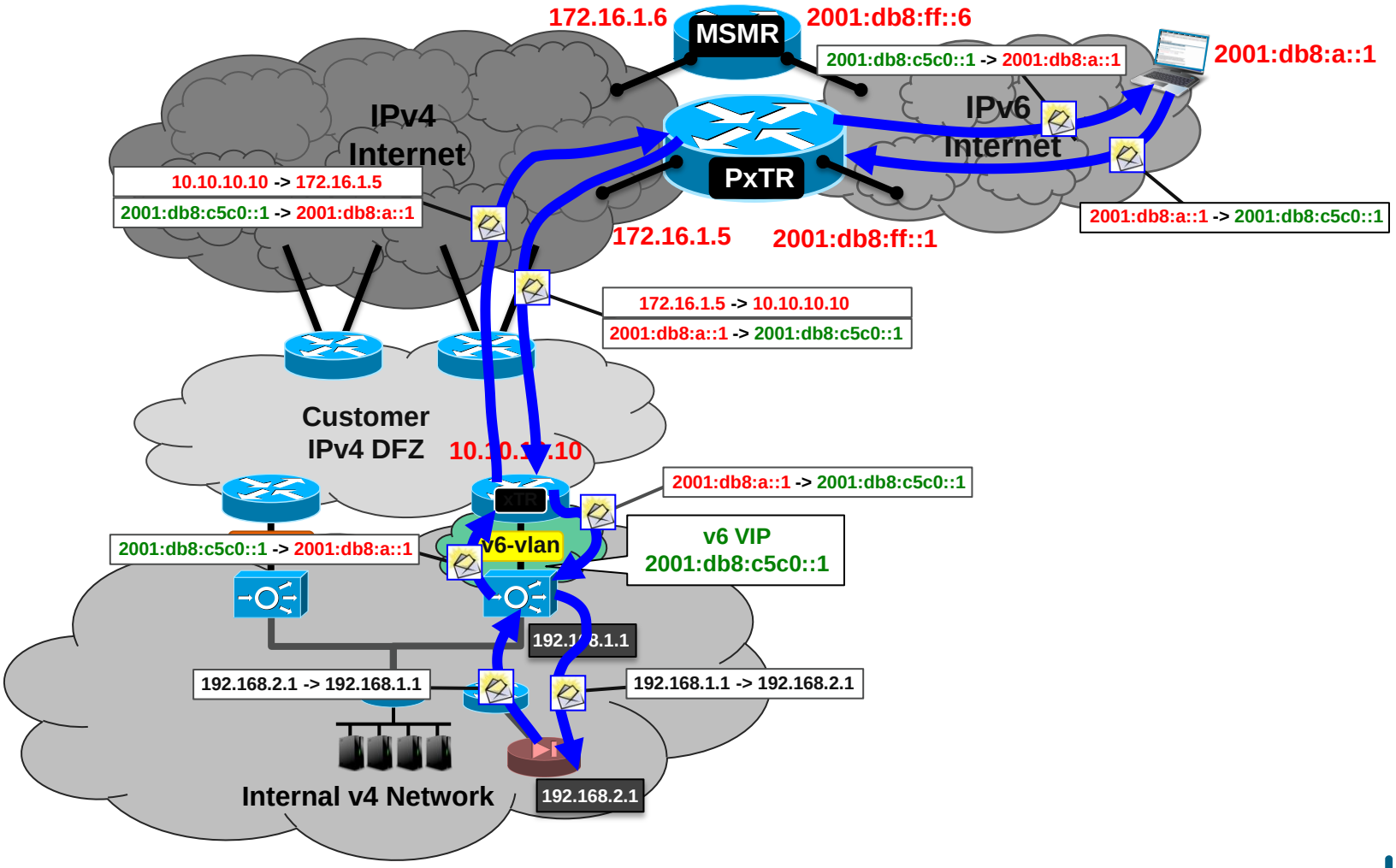
LISP Use Cases – IPv6 Migration Support
Customer Case Study – LISP Configuration



LISP Use Cases – IPv6 Migration Support
Customer Case Study – Packet Flow example



LISP Use Cases – IPv6 Migration Support
Customer Case Study – Example Packet Flow



LISP Use Cases
IPv6 Transition Support

Applicability:

- Low CapEx, Quick, IPv6 Web Presence
- Useful in all other LISP Use Cases (Multi-homing, VM-mobility, Virtualization…)

Customers/EFTs

- Cisco IT
- Facebook
- Qualcomm
- InTouch
- Deutsche Bank
- Munich Airport
- IsarNet

World IPv6 Day Sites using LISP

Cisco
lisp.cisco.com (AAAA: 2610:d0:110c:1::3, ::4)
Facebook
www.lisp6.facebook.com (AAAA: 2610:D0:FACE::9)
Qualcomm
www.ipv6.eudora.com (AAAA: 2610:d0:120d::10)
jobs.qualcomm.com (no longer AAAA)
Deutsche Bank
www.ipv6-db.com (AAAA: 2610:d0:2113:3::3)
Munich Airport
lisp.munich-airport.de (no longer AAAA)
Isarnet
lisp.isarnet.net (AAAA: 2610:d0:211f:fffe::101)
InTouch
www.lisp.intouch.eu (AAAA: 2610:d0:210f:100::101)

World IPv6 Day Sites Statistics (and current)

http://honeysuckle.noc.ucla.edu/cgi-bin/smokeping.cgi?target=LISP

Facebook IPv6 Experience with LISP

http://nanog.org/meetings/nanog50/presentations/Tuesday/NANOG50.Talk9.lee_nanog50_atlanta_oct2010_007_publish.pdf

LISP Use Cases – Network Virtualization

Layer 3 Virtualization Options

- VRF Lite
- VRF Lite over IP (GRE)
- VRF Lite over DMVPN/GET-VPN
- MPLS VPN
- MPLS VPN over IP (GRE)
- MPLS VPN over DMVPN
- MPLS VPN over Multipoint GRE (mGRE)
- **Virtualization with LISP**

Network Virtualization with LISP
Segmentation

LISP Virtualization

- A technique to Virtualized the EID and RLOC namespaces
- The LISP Instance-ID is the mechanism to separate address spaces in the control and data planes

Instance-ID

- a 24-bit unstructured number
- Data-plane: in LISP encapsulation header
- Control-plane: EID encoded in LCAF format

LISP Use Cases
Virtualization/Multi-Tenancy

Needs:

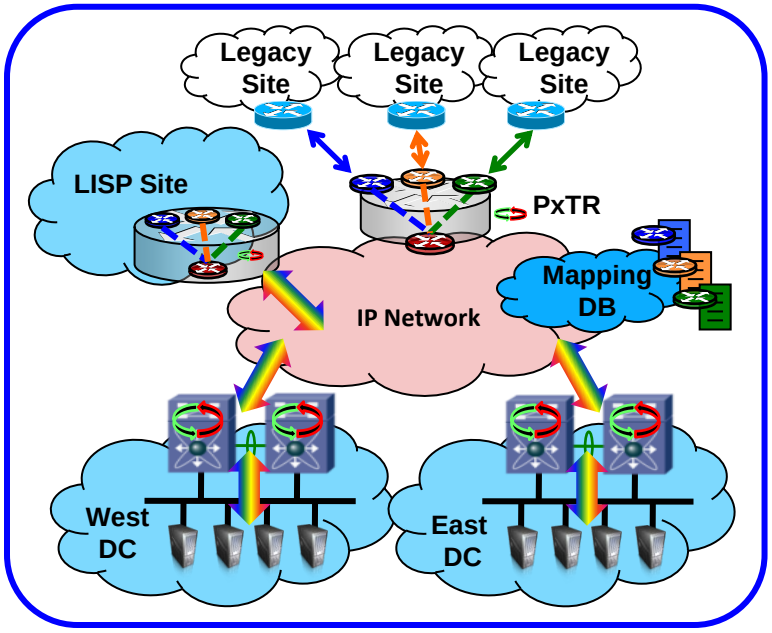
- Integrated Segmentation
- Minimal Infrastructure disruption
- Global scale and interoperability

LISP Solution:

- 24-bit LISP instance-ID segments control plane and data plane mappings
- VRF mappings to instance-id

Benefits:

- Very high scale tenant segmentation
- Global mobility + high scale segmentation integrated in single IP solution
- IP based solution, transport independent
- No Inter-AS complexity
- Overlay solution transparent to the core



Applicability:

- Multi-provider Core
- Encryption can be added

Customers/EFTs:

- Tier 1 ISP
- Major Health Care Provider

LISP – Data Format Example
IPv4 EID/IPv4 RLOC Example

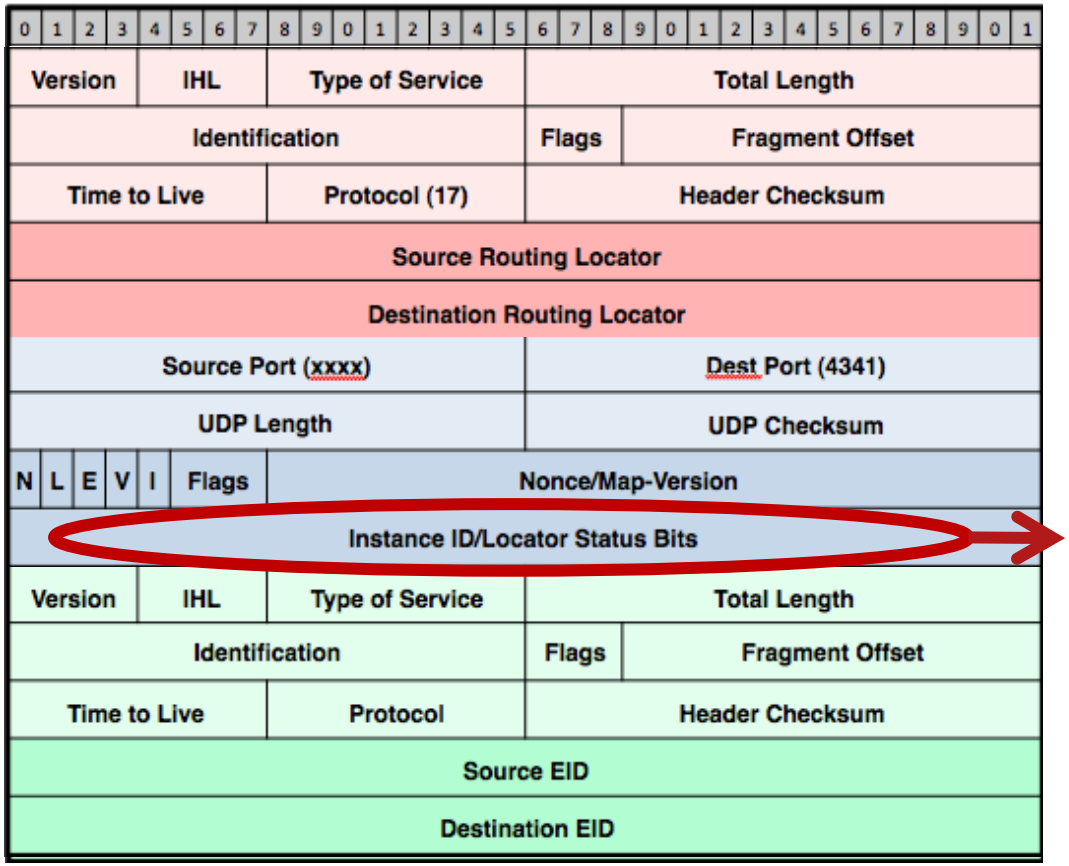
draft-ietf-lisp-15

IPv4 Outer Header: Router supplies RLOCs

UDP

LISP header

IPv4 Inner Header: Host supplies EIDs



Instance ID Maps Aligns with VRF Definition

‘Instance-id’ Command

eid-table

To configure a LISP instance-id for association with a virtual routing and forwarding (VRF) table or default table through which the EID address space is reachable, use the **eid-table command in LISP configuration mode. To**

remove this association, use the **no form of this command.**

[no] eid-table {default | {vrf *vrf-name}} instance-id iid

Syntax Description

Default

Select the default (global) routing table for association with the configured instance-id.

vrf *vrf-name*

Select the VRF named vrf-name for association with the configured instance-id.

instance-id *iid*

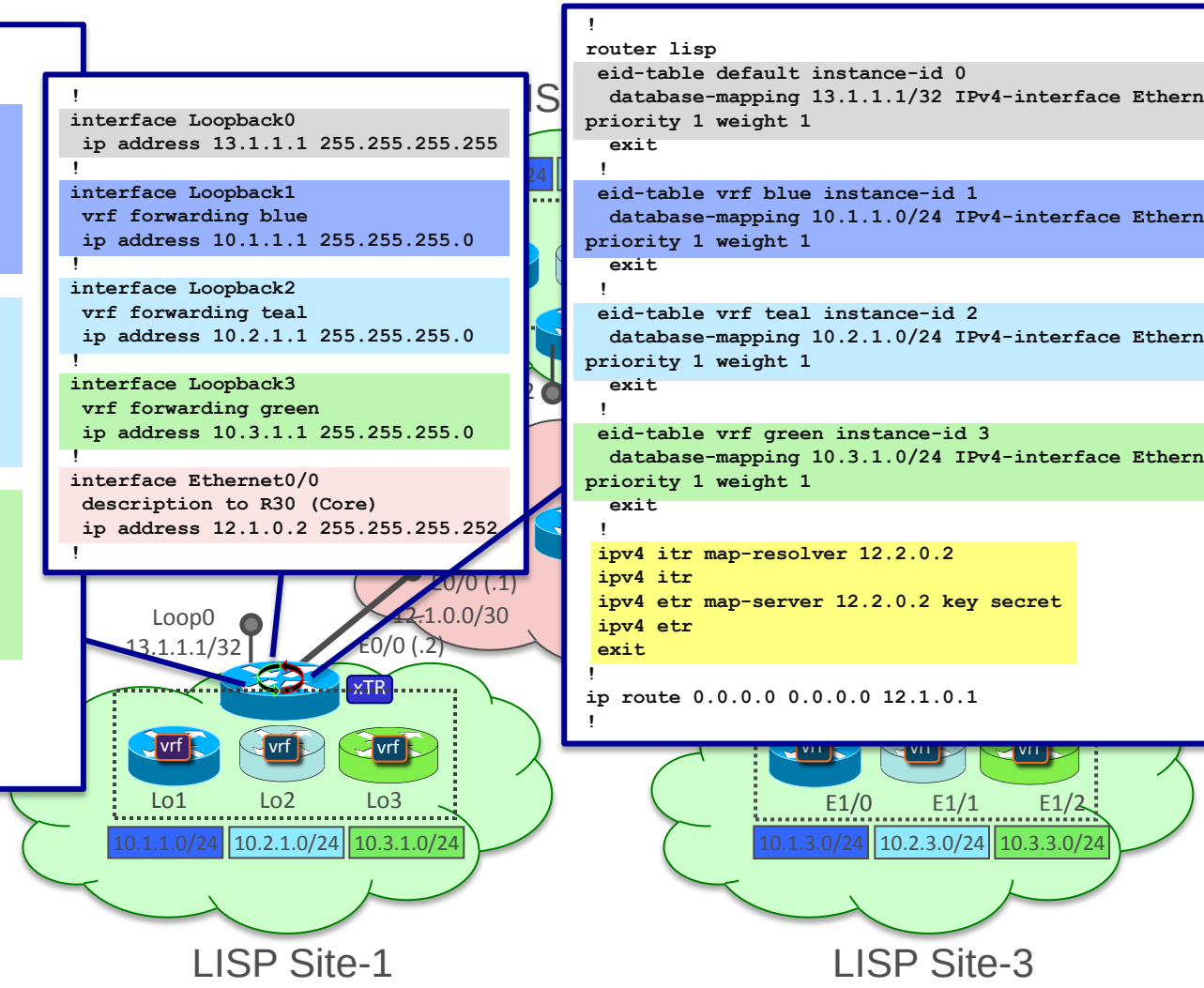
The instance-id to be associated with this eid-table (value between 0 and 16777215)

LISP Use-Cases – Multi-Tenancy
Case Study – Configuration Example

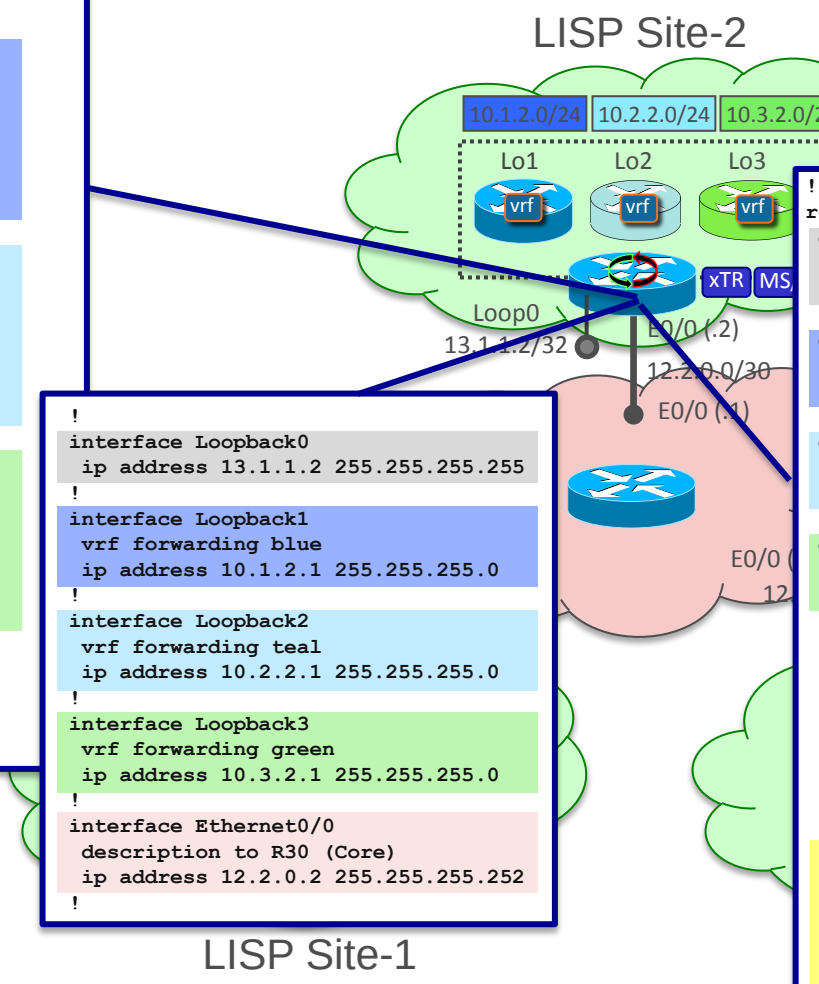
```
!
hostname xTR-1
!
vrf definition blue
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition teal
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition green
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
```

```
!
interface Loopback0
 ip address 13.1.1.1 255.255.255.255
!
interface Loopback1
 vrf forwarding blue
 ip address 10.1.1.1 255.255.255.0
!
interface Loopback2
 vrf forwarding teal
 ip address 10.2.1.1 255.255.255.0
!
interface Loopback3
 vrf forwarding green
 ip address 10.3.1.1 255.255.255.0
!
interface Ethernet0/0
 description to R30 (Core)
 ip address 12.1.0.2 255.255.255.252
!
```

```
!
router lisp
 eid-table default instance-id 0
  database-mapping 13.1.1.1/32 IPv4-interface Ethernet0/0
priority 1 weight 1
  exit
 !
 eid-table vrf blue instance-id 1
  database-mapping 10.1.1.0/24 IPv4-interface Ethernet0/0
priority 1 weight 1
  exit
 !
 eid-table vrf teal instance-id 2
  database-mapping 10.2.1.0/24 IPv4-interface Ethernet0/0
priority 1 weight 1
  exit
 !
 eid-table vrf green instance-id 3
  database-mapping 10.3.1.0/24 IPv4-interface Ethernet0/0
priority 1 weight 1
  exit
 !
 ipv4 itr map-resolver 12.2.0.2
 ipv4 itr
 ipv4 etr map-server 12.2.0.2 key secret
 ipv4 etr
 exit
!
ip route 0.0.0.0 0.0.0.0 12.1.0.1
!
```



LISP Use-Cases – Multi-Tenancy
Case Study – Configuration Example




```
!
hostname xTR-2
!
vrf definition blue
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition teal
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition green
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
```

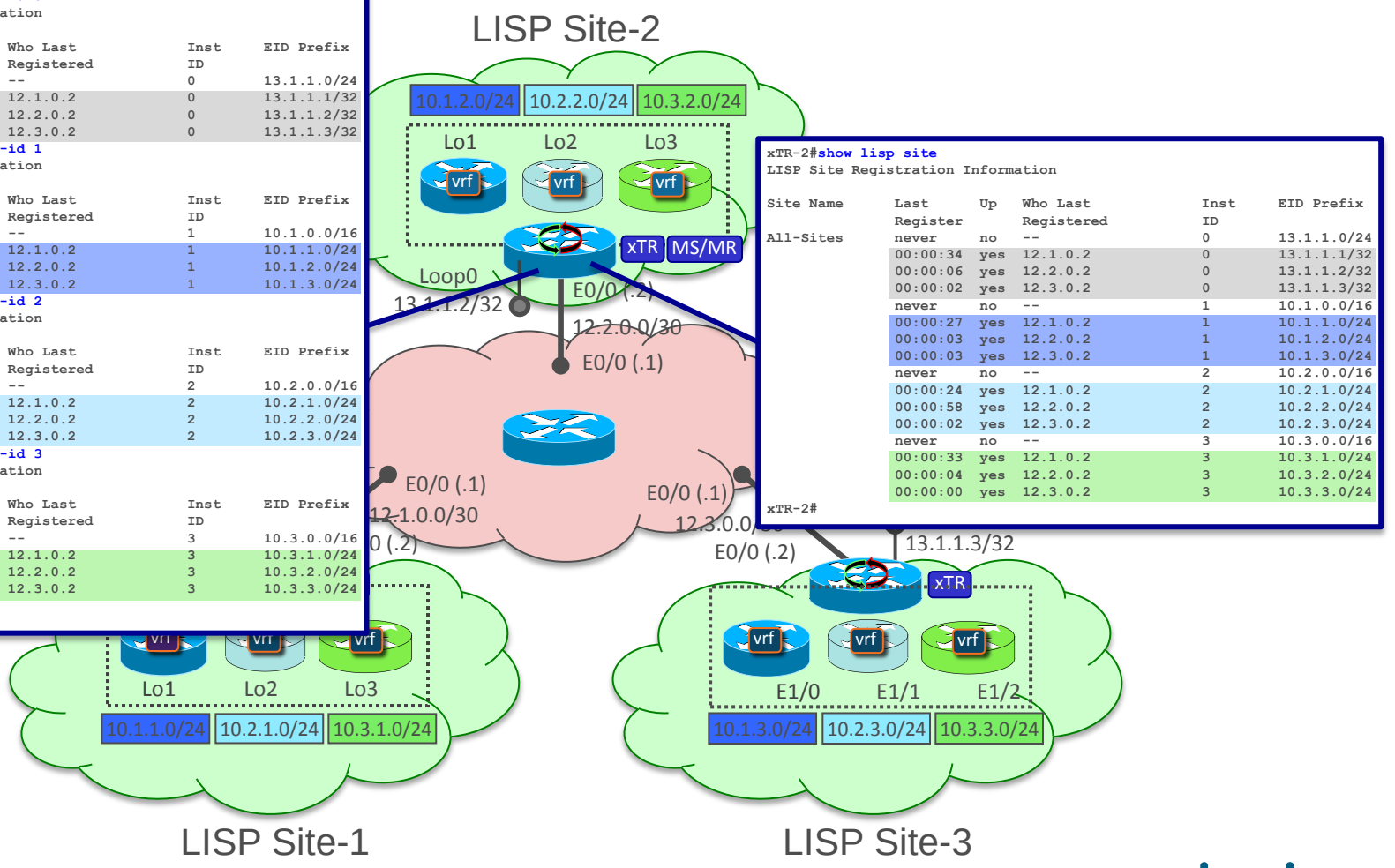
```
!
interface Loopback0
 ip address 13.1.1.2 255.255.255.255
!
interface Loopback1
 vrf forwarding blue
 ip address 10.1.2.1 255.255.255.0
!
interface Loopback2
 vrf forwarding teal
 ip address 10.2.2.1 255.255.255.0
!
interface Loopback3
 vrf forwarding green
 ip address 10.3.2.1 255.255.255.0
!
interface Ethernet0/0
 description to R30 (Core)
 ip address 12.2.0.2 255.255.255.252
!
```

```
!
router lisp
 eid-table default instance-id 0
  database-mapping 13.1.1.2/32 12.2.0.2 priority 1 weight 1
  exit
 !
 eid-table vrf blue instance-id 1
  database-mapping 10.1.2.0/24 12.2.0.2 priority 1 weight 1
  exit
 !
 eid-table vrf teal instance-id 2
  database-mapping 10.2.2.0/24 12.2.0.2 priority 1 weight 1
  exit
 !
 eid-table vrf green instance-id 3
  database-mapping 10.3.2.0/24 12.2.0.2 priority 1 weight 1
  exit
 !
 site All-Sites
  authentication-key secret
  eid-prefix 13.1.1.0/24 accept-more-specifics
  eid-prefix instance-id 1 10.1.0.0/16 accept-more-specifics
  eid-prefix instance-id 2 10.2.0.0/16 accept-more-specifics
  eid-prefix instance-id 3 10.3.0.0/16 accept-more-specifics
  exit
 !
 ipv4 map-server
 ipv4 map-resolver
 ipv4 itr map-resolver 12.2.0.2
 ipv4 itr
 ipv4 etr map-server 12.2.0.2 key secret
 ipv4 etr
 exit
!
```

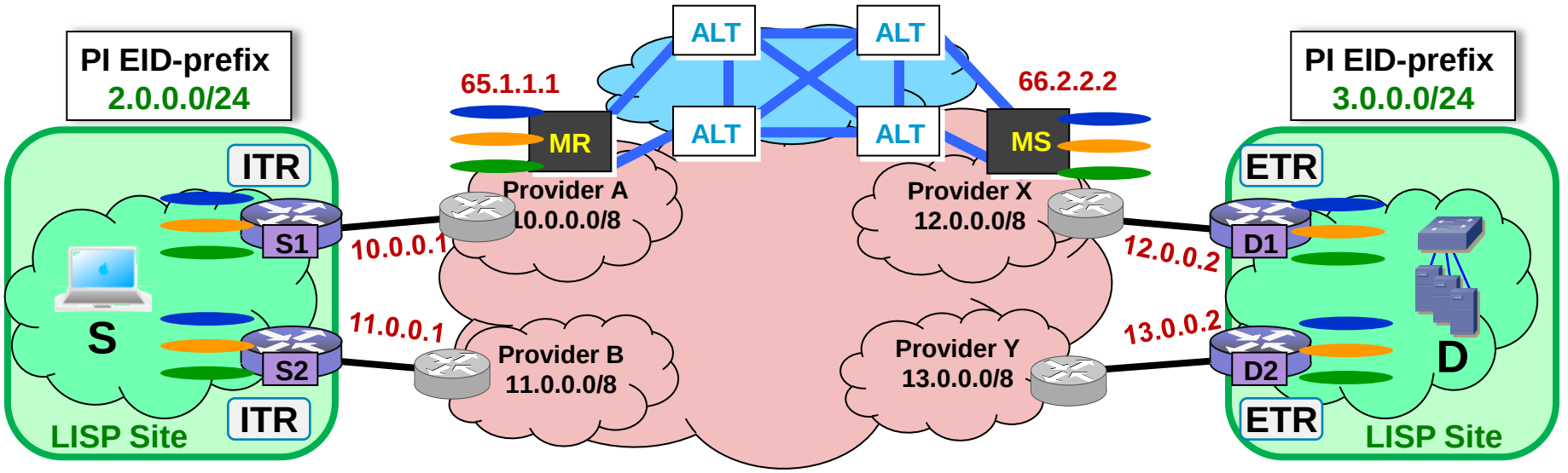
LISP Use-Cases – Multi-Tenancy
Case Study – CLI Output

```
xTR-2#show lisp site instance-id 0
LISP Site Registration Information

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
All-Sites      never     no   --                0        13.1.1.0/24
               00:00:48  yes  12.1.0.2          0        13.1.1.1/32
               00:00:20  yes  12.2.0.2          0        13.1.1.2/32
               00:00:18  yes  12.3.0.2          0        13.1.1.3/32
xTR-2#show lisp site instance-id 1
LISP Site Registration Information

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
All-Sites      never     no   --                1        10.1.0.0/16
               00:00:43  yes  12.1.0.2          1        10.1.1.0/24
               00:00:22  yes  12.2.0.2          1        10.1.2.0/24
               00:00:19  yes  12.3.0.2          1        10.1.3.0/24
xTR-2#show lisp site instance-id 2
LISP Site Registration Information

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
All-Sites      never     no   --                2        10.2.0.0/16
               00:00:43  yes  12.1.0.2          2        10.2.1.0/24
               00:00:19  yes  12.2.0.2          2        10.2.2.0/24
               00:00:21  yes  12.3.0.2          2        10.2.3.0/24
xTR-2#show lisp site instance-id 3
LISP Site Registration Information

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
All-Sites      never     no   --                3        10.3.0.0/16
               00:00:56  yes  12.1.0.2          3        10.3.1.0/24
               00:00:28  yes  12.2.0.2          3        10.3.2.0/24
               00:00:25  yes  12.3.0.2          3        10.3.3.0/24
xTR-2#
```

```
xTR-2#show lisp site
LISP Site Registration Information

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
All-Sites      never     no   --                0        13.1.1.0/24
               00:00:34  yes  12.1.0.2          0        13.1.1.1/32
               00:00:06  yes  12.2.0.2          0        13.1.1.2/32
               00:00:02  yes  12.3.0.2          0        13.1.1.3/32
               never     no   --                1        10.1.0.0/16
               00:00:27  yes  12.1.0.2          1        10.1.1.0/24
               00:00:03  yes  12.2.0.2          1        10.1.2.0/24
               00:00:03  yes  12.3.0.2          1        10.1.3.0/24
               never     no   --                2        10.2.0.0/16
               00:00:24  yes  12.1.0.2          2        10.2.1.0/24
               00:00:58  yes  12.2.0.2          2        10.2.2.0/24
               00:00:02  yes  12.3.0.2          2        10.2.3.0/24
               never     no   --                3        10.3.0.0/16
               00:00:33  yes  12.1.0.2          3        10.3.1.0/24
               00:00:04  yes  12.2.0.2          3        10.3.2.0/24
               00:00:00  yes  12.3.0.2          3        10.3.3.0/24
xTR-2#
```



LISP Use Case – Multi-Tenancy
Network Virtualization "Over the Top"



- Allows network segmentation on xTR (CE to SP)
- PE routers require minimal routes (RLOC address only)
- VRF Segmentation is applied to CE/xTR
- SP PE has minimal customer routes (ideal if Enterprise PE)
- CE/xTR can add additional customer (per VRF), and routes are hidden from SP network.
- Can add GET VPN for additional data security (IPSec)

VRFs

Legend:
EIDs -> Green
Locators -> Red
BGP-over-GRE
Physical link

LISP Use Cases
VM-Mobility

Needs:

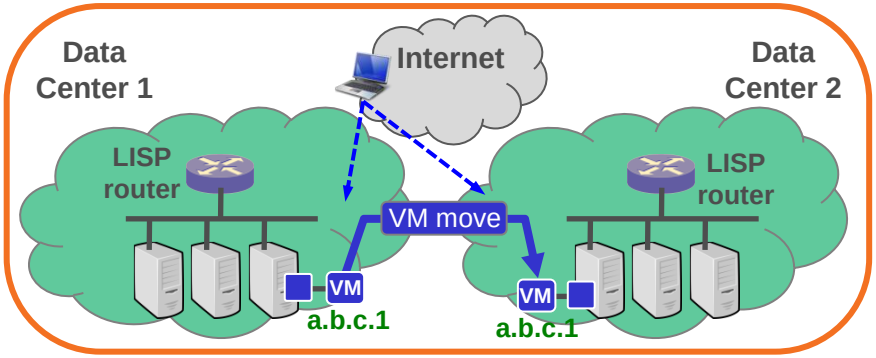
- VM-Mobility across subnets
- Move detection, dynamic EID-to-RLOC mappings, traffic redirection

LISP Solution:

- OTV + LISP to extend subnets
- LISP for VM-moves across subnets

Benefits:

- Integrated Mobility
- Direct Path (no triangulation)
- Connections maintained across moves
- No routing re-convergence
- No DNS updates required
- Global Scalability (cloud bursting)
- IPv4/IPv6 Support
- ARP elimination



Applicability:

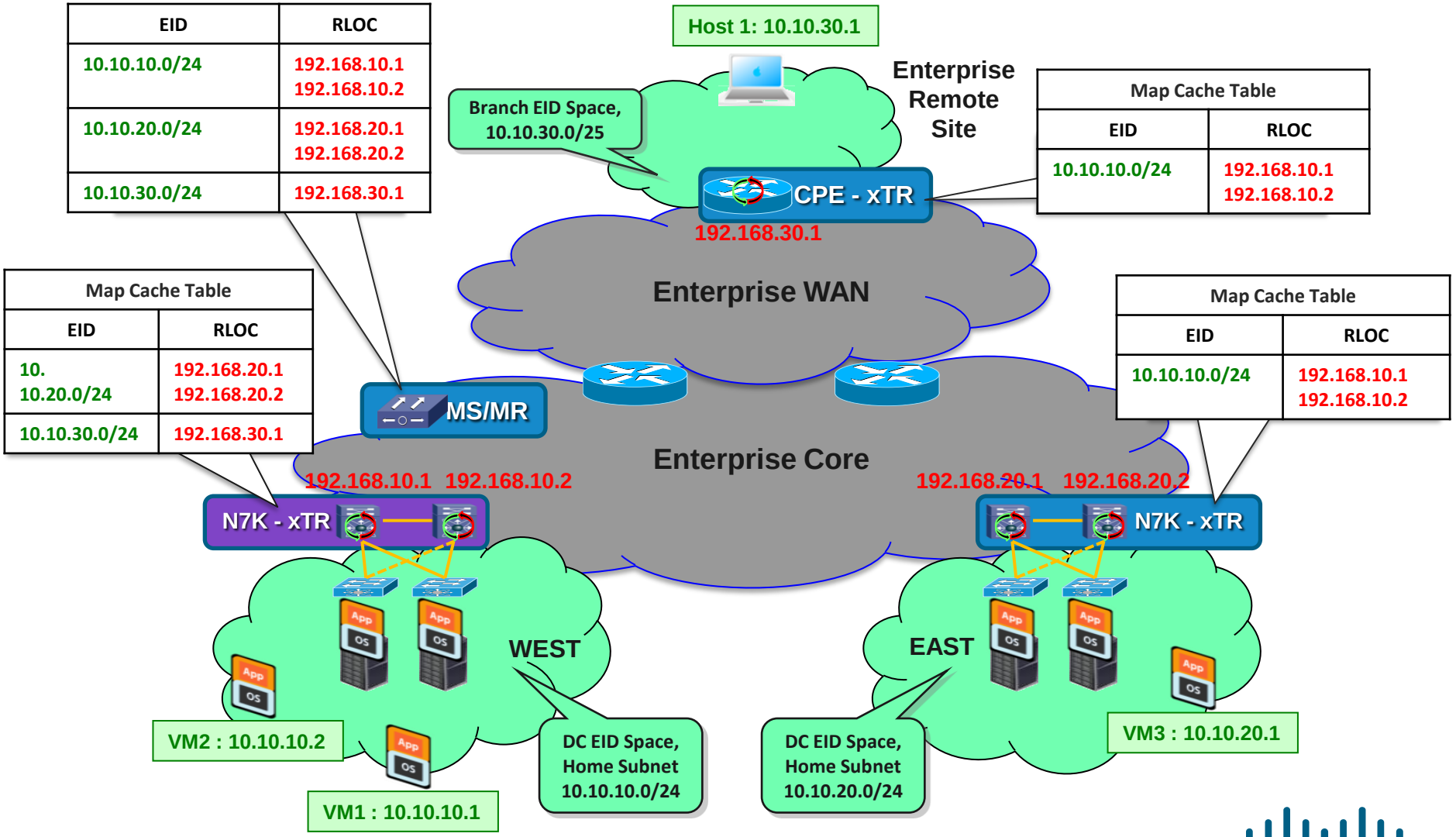
- VM OS agnostic
- Services Creation (disaster recovery, cloud burst, etc.)

Customers/EFTs:

- Cisco IT
- Qualcomm
- More…

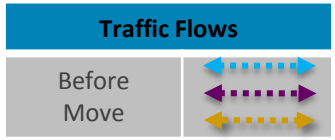
LISP Use Cases – VM-Mobility

Case Study – Topology, Initial Map Cache entries



LISP Use Cases – VM-Mobility

Case Study – traffic flows before move



EID	RLOC
10.10.10.0/24	192.168.10.1 192.168.10.2
10.10.20.0/24	192.168.20.1 192.168.20.2
10.10.30.0/24	192.168.30.1

Host 1: 10.10.30.1

Enterprise Remote Site

Branch EID Space, 10.10.30.0/25

10.10.30.1<->10.10.10.1

CPE - xTR

192.168.30.1

Map Cache Table	
EID	RLOC
10.10.10.0/24	192.168.10.1 192.168.10.2

Enterprise WAN

192.168.30.1<->192.168.10.2

10.10.30.1<->10.10.10.1

Map Cache Table	
EID	RLOC
10. 10.20.0/24	192.168.20.1 192.168.20.2
10.10.30.0/24	192.168.30.1

MS/MR

192.168.20.2<->192.168.10.2

10.10.20.1<->10.10.10.1

Enterprise

Map Cache Table	
EID	RLOC
10.10.10.0/24	192.168.10.1 192.168.10.2

192.168.10.1 192.168.10.2

192.168.20.1 192.168.20.2

N7K - xTR

N7K - xTR

10.10.10.2<->10.10.10.1

10.10.30.1<->10.10.10.1

10.10.20.1<->10.10.10.1

10.10.20.1<->10.10.10.1

WEST

EAST

VM2 : 10.10.10.2

VM1 : 10.10.10.1

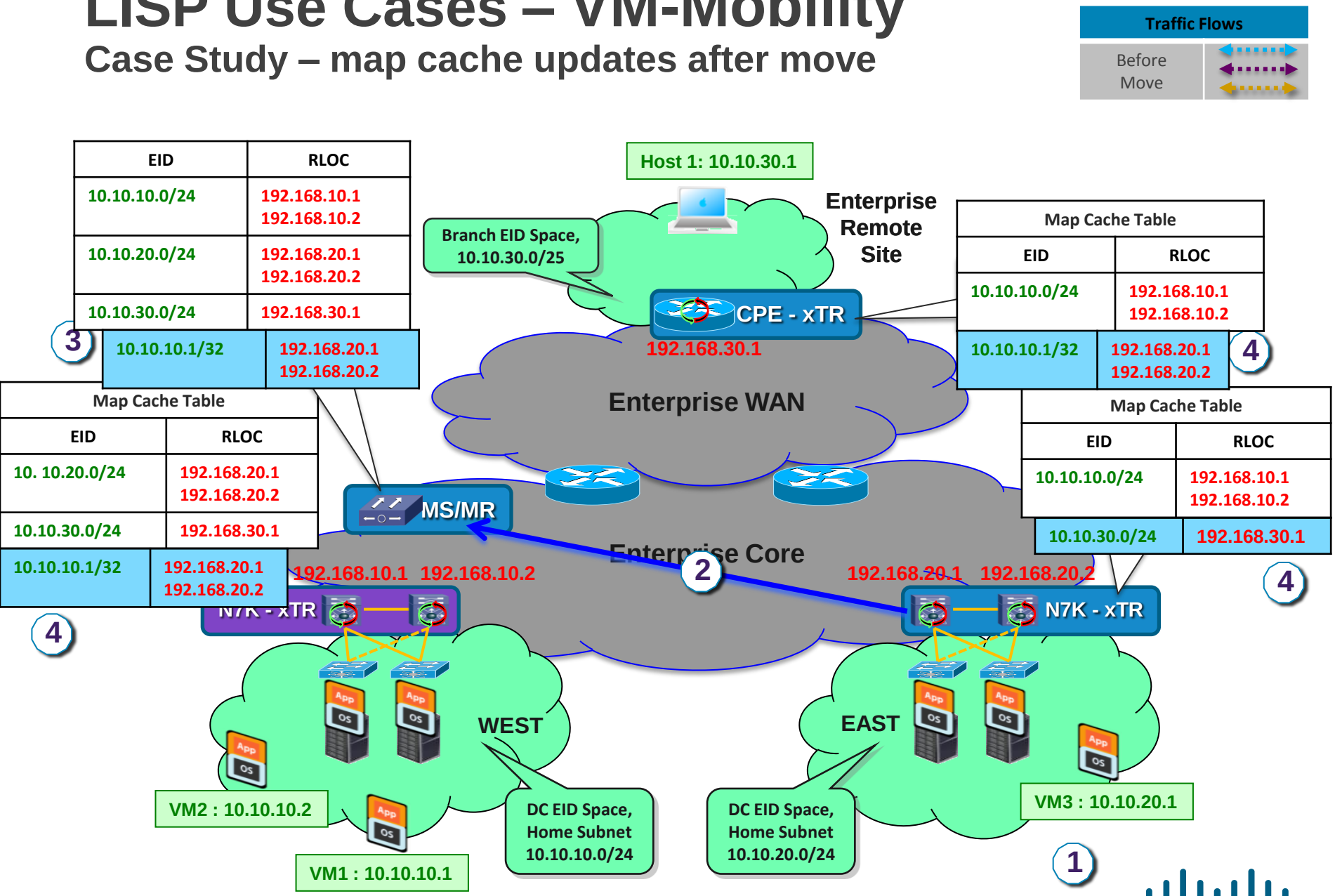
DC EID Space, Home Subnet 10.10.10.0/24

DC EID Space, Home Subnet 10.10.20.0/24

VM3 : 10.10.20.1

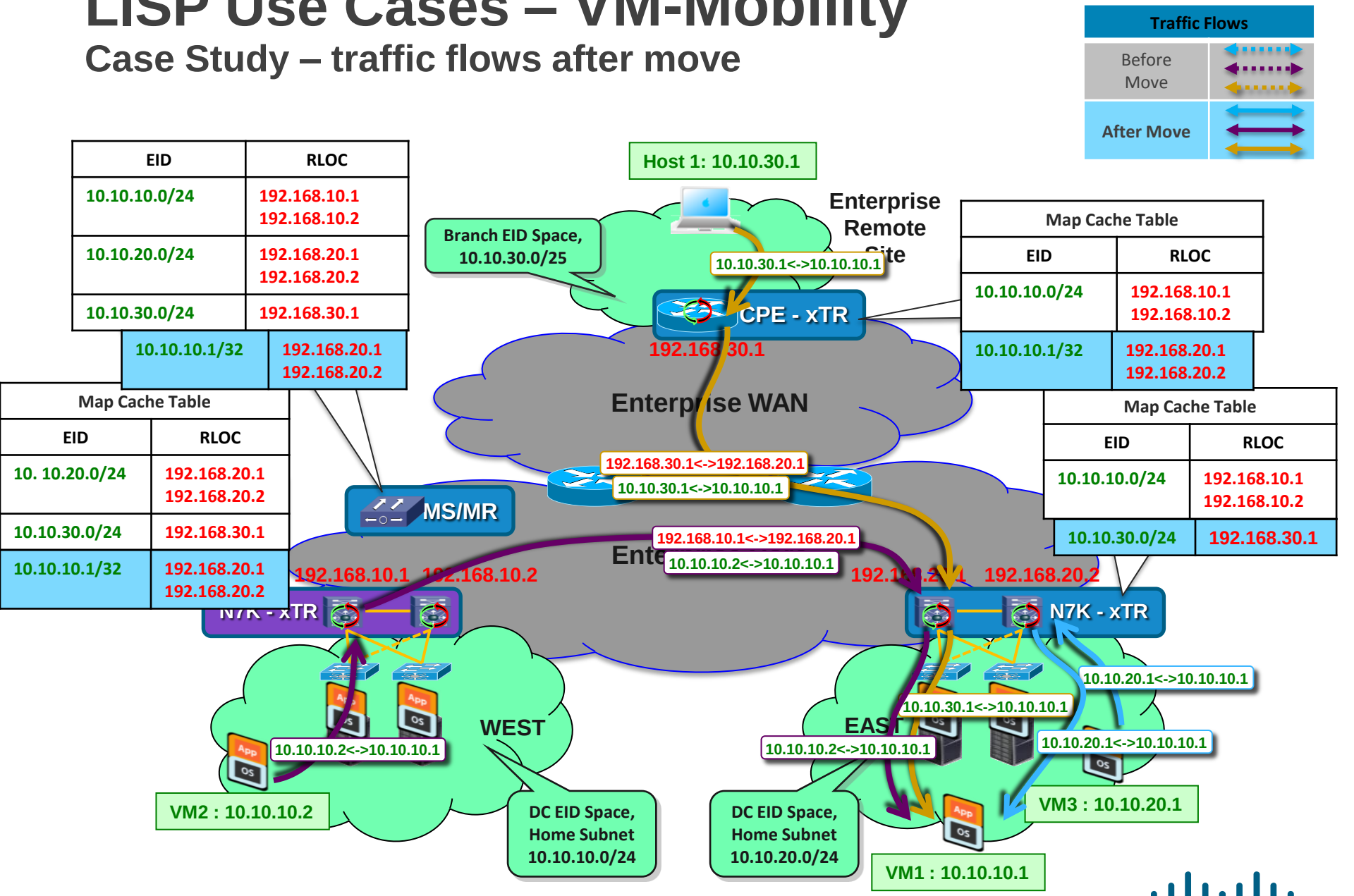
LISP Use Cases – VM-Mobility

Case Study – map cache updates after move



LISP Use Cases – VM-Mobility

Case Study – traffic flows after move



‘lisp dynamic-eid roamer’ Command

lisp dynamic-eid

To configure a LISP VM-Mobility (dynamic-EID roaming) policy and enter dynamic-EID configuration mode on an

Syntax Description

dynamic-EID-policy-name

The name of the LISP dynamic-EID policy.

database-mapping

To configure a IPv4 or IPv6 dynamic-EID-to-RLOC mapping relationship and its associated traffic policy use the

Syntax Description

dynamic-EIDprefix

The IPv4 or IPv6 dynamic-EID prefix and length to be registered as a roaming EID for this policy.

Example:

lisp dynamic-eid Roamer-1

database-mapping 172.16.1.1/32 10.1.1.1 priority 1 weight 100

LISP Use Cases
LISP Mobile Node

Needs:

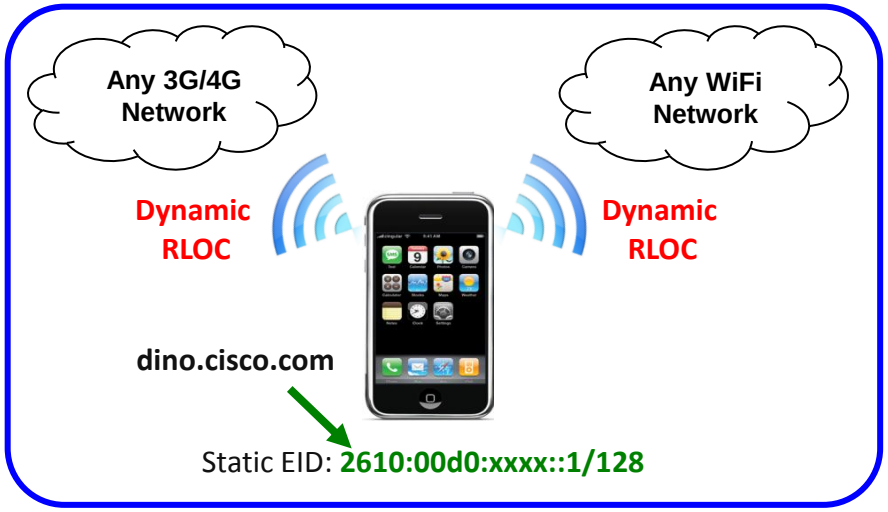
- Mobile devices roaming across any access media without connection reset
- Mobile device keeps the same IP address forever

LISP Solution:

- LISP level or indirection separates endpoints and locators
- Network-based; no host changes, minimal network changes
- Scalable, host-level registration (10^{10})

Benefits:

- MNs can roam and stay connected
- MNs can be servers
- MNs roam without DNS changes
- MNs can use multiple interfaces
- Packets have “stretch-1” reducing latency



Applicability:

- IPv4 and IPv6
- Android and Linux
- Open

Customers/EFTs:

- Major vehicle manufacturer
- A wireless provider

Standardization

LISP Standardization Effort
Open Design

IETF LISP WG: http://tools.ietf.org/wg/lisp/

AD = Area Director Evaluation

Draft	Next Steps/Target
LISP base protocol (draft-ietf-lisp-15)	AD Evaluation…
LISP+ALT (draft-ietf-lisp-alt-07)	AD Evaluation…
LISP Interworking (draft-ietf-lisp-interworking-02)	Publication Requested…
LISP Map Server (draft-ietf-lisp-ms-11)	AD Evaluation…
LISP Multicast (draft-ietf-lisp-multicast-07)	AD Evaluation…
LISP Internet Groper (draft-ietf-lisp-lig-05)	IESG Evaluation… Open source versions available
LISP Mobile Node (draft-meyer-lisp-mn-05)	Three prototype implementations underway Not WG Document
LISP Canonical Address Format (draft-farinacci-lisp-lcaf-05)	-05 update sent to WG list Proposed for WG adoption
LISP MIB (draft-ietf-lisp-mib-02)	Active…
LISP Map Versioning (draft-ietf-lisp-map-versioning-02)	Last Call…

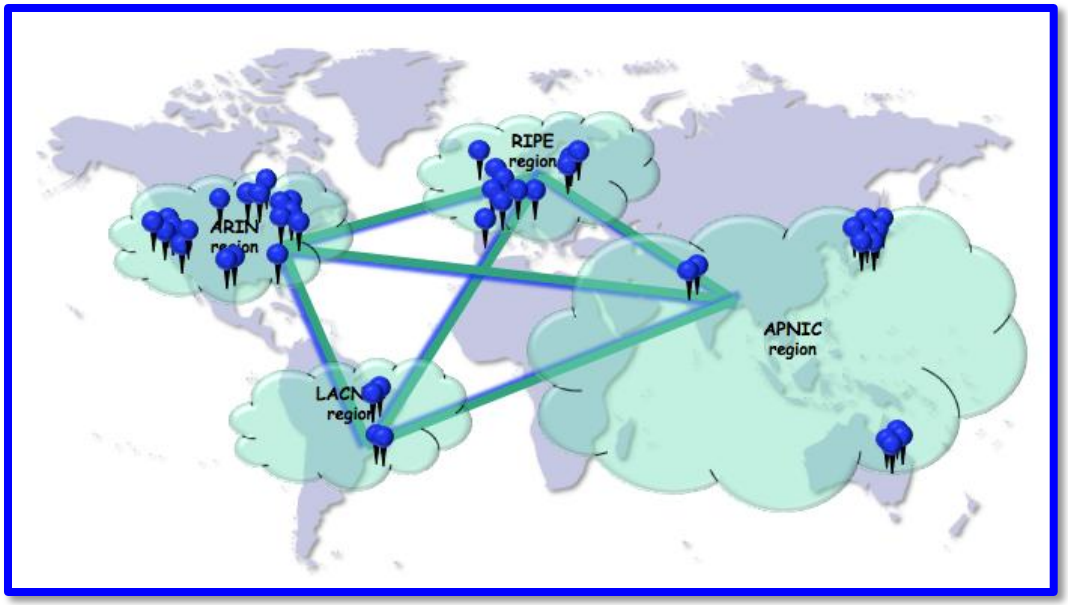
LISP Deployments
International LISP Beta Network

LISP Community Operated

- ~ 4 years operational
- > **130+ sites, 25 countries**

Nine implementations deployed today…

- Cisco: IOS, IOS-XE, NX-OS
- FreeBSD: OpenLISP
- OpenWrt
- Linux
- Android (Gingerbread)
- Two other router vendor



cisco
http://www.lisp4.net
http://lisp.cisco.com

InTouch
http://www.lisp.intouch.eu/

facebook
http://www.lisp6.facebook.com

isarNet Professional Networking
http://lisp.isarnet.net/

QUALCOMM
http://www6.eudora.com
http://myvpn6.qualcomm.com

Google Microsoft VeriSign verizon
UCLA NEW YORK UNIVERSITY
and more…

LISP – A Routing Architecture; Not a Feature
LISP Innovations

Enables **IP Number Portability**

- With session survivability
- Never change host IP addresses
  No renumbering costs
- No DNS "name -> EID" binding change

Uses **pull** vs. **push** routing

- OSPF and BGP are **push** models; routing stored in the forwarding plane
- LISP is a **pull** model; Analogous to DNS; massively scalable

An **over-the-top** technology

- Address Family agnostic
- Incrementally deployable
- No changes in end systems

Creates a **Level of Indirection**

- Separates End-Host and Site addresses

Deployment **simplicity**

- No host changes
- Minimal CPE changes
- Some new core infrastructure components

Enables other **interesting features**

- Simplified multi-homing with Ingress traffic engineering – without the need for BGP
- End-host mobility without renumbering
- Address Family agnostic support

An **Open Standard**

- No Cisco Intellectual Property Rights

LISP References
Resources

LISP Information

- IETF LISP WG — http://tools.ietf.org/wg/lisp/
- LISP Beta Network — http://www.lisp4.net or http://www.lisp6.net
- Cisco LISP Site — http://lisp.cisco.com (v4 and v6)
- Cisco LISP Marketing — http://www.cisco.com/go/lisp

Mailing Lists

- IETF LISP WG — lisp@ietf.org
- LISP Interest (public) — lisp-interest@puck.nether.net
- Cisco LISP Questions — lisp-support@cisco.com

Thank you.

Backup

LISP Overview

LISP Overview
What is the problem with an "overloaded" semantic?

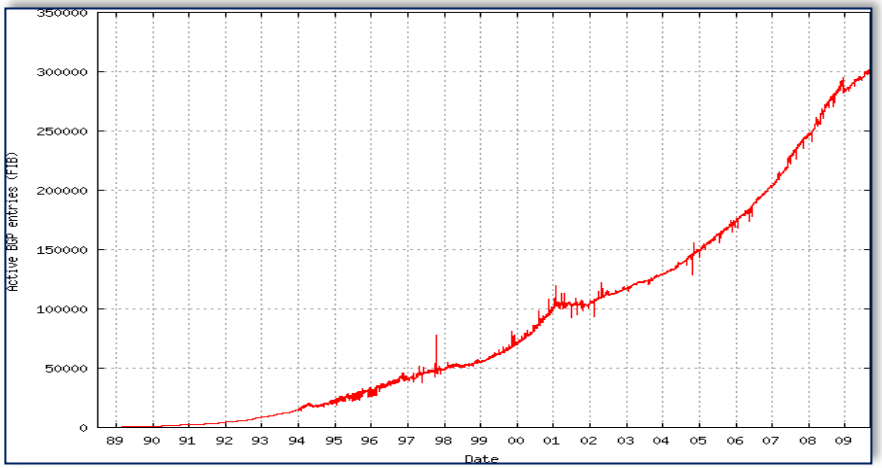
- Loc/ID overload leads to Internet scaling issues

  Why do current IP semantics cause scaling issues?

  - Overloaded IP address semantic makes efficient routing impossible
  - Today, "addressing follows topology," which limits route aggregation compactness
  - IPv6 does not fix this

  Why are route scaling issues bad?

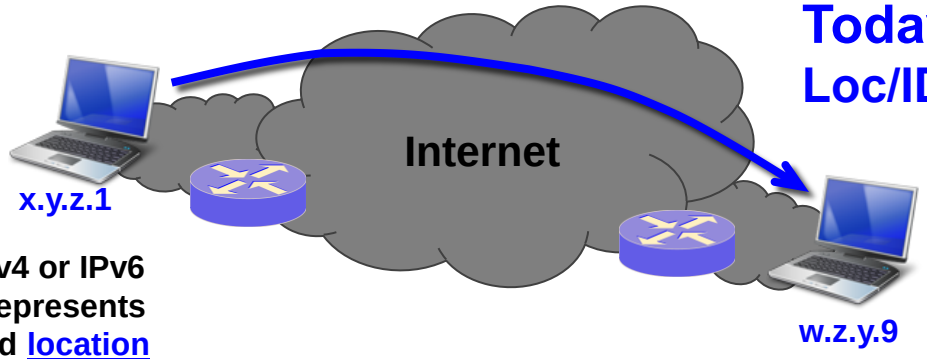
  - Routers require tons of expensive memory to hold the Internet Routing Table in the forwarding plane
  - It's expensive for network builders/operators
  - Replacing equipment for the wrong reason (to hold the routing table); replacement should be toimplement new features



"… routing scalability is the most important problem facing the Internet today and must be solved …"

Internet Architecture Board (IAB)
October 2006 Workshop (written as RFC 4984)

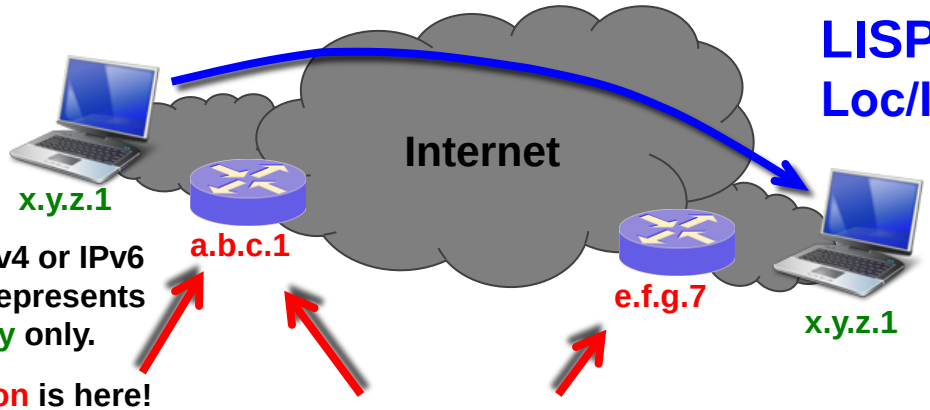
LISP Overview
What do we mean by “location” and “identity”?



Today’s Internet Behavior
Loc/ID “overloaded” semantic

Device IPv4 or IPv6 address represents identityand location

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



LISP Behavior
Loc/ID “split”

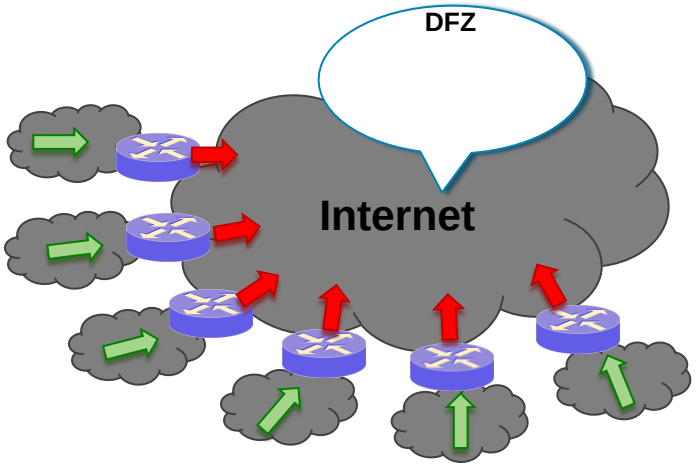
Device IPv4 or IPv6 address represents identity only.

Its location is here!

Only the location changes

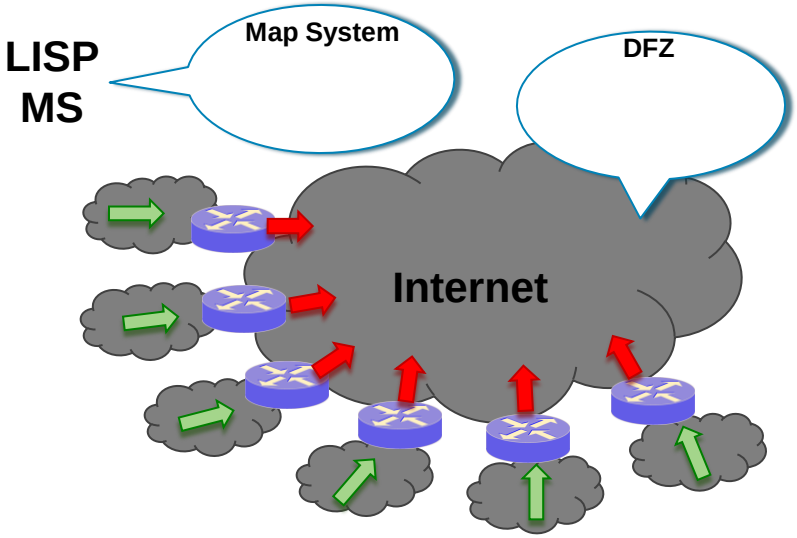
When the device moves, keeps its IPv4 or IPv6 address. It has the same identity

LISP Overview
How does Location/ID Split help solve this problem?



Today's Internet Behavior
Loc/ID "overload"

In this model, everything goes in the DFZ



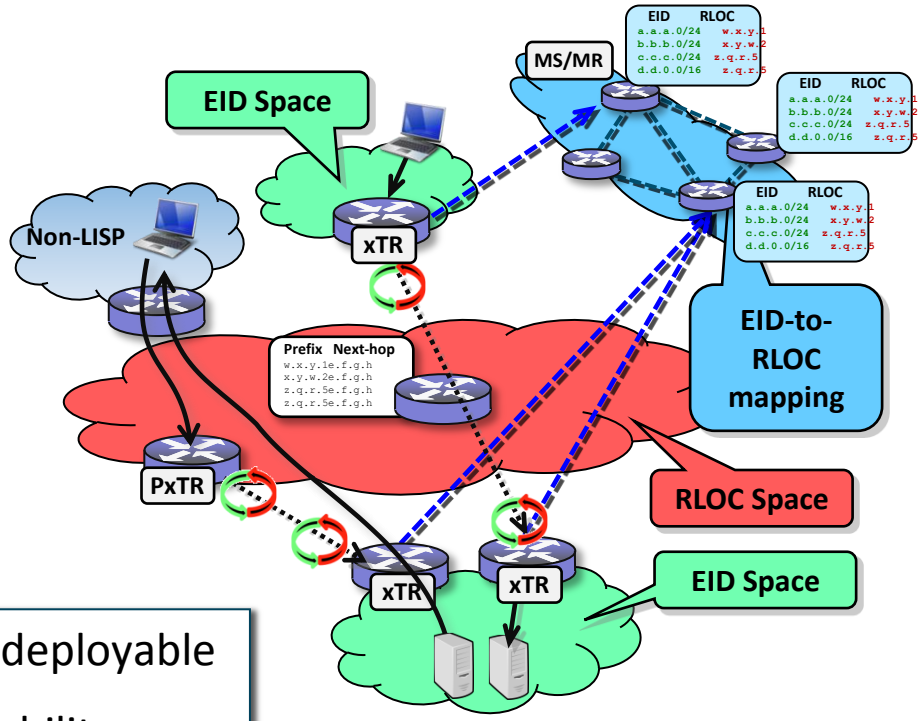
LISP Behavior
Loc/ID "split"

In this model, only RLOCs go in the DFZ;
EIDs go in the LISP Mapping System!

LISP Overview
A "level of indirection"

LISP creates a "Level of indirection" with two namespaces: **EID** and **RLOC**

- **EID (Endpoint Identifier)** is the IP address of a host – just as it is today
- **RLOC (Routing Locator)** is the IP address of the LISP router for the host
- **EID-to-RLOC mapping** is the distributed architecture that maps **EIDs** to **RLOCs**



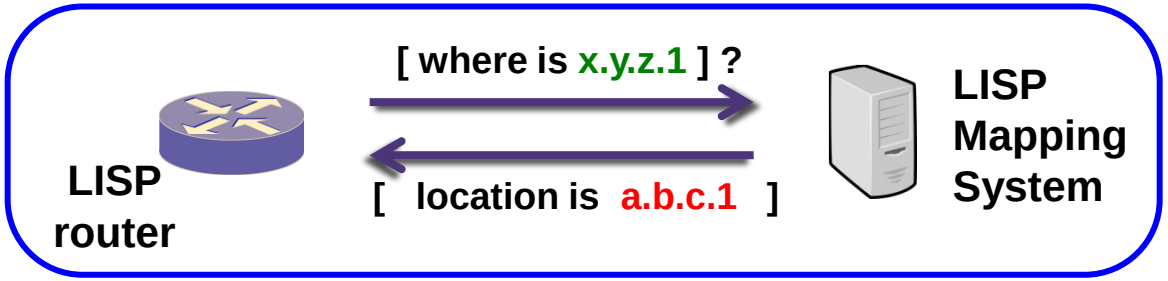
- Network-based solution
- Incrementally deployable
- No host changes
- Support for mobility
- Minimal configuration
- Address Family agnostic

LISP Overview
LISP Mapping Resolution – DNS analog

LISP Map Lookup is analogous to a DNS lookup

- DNS resolves IP addresses for URLs

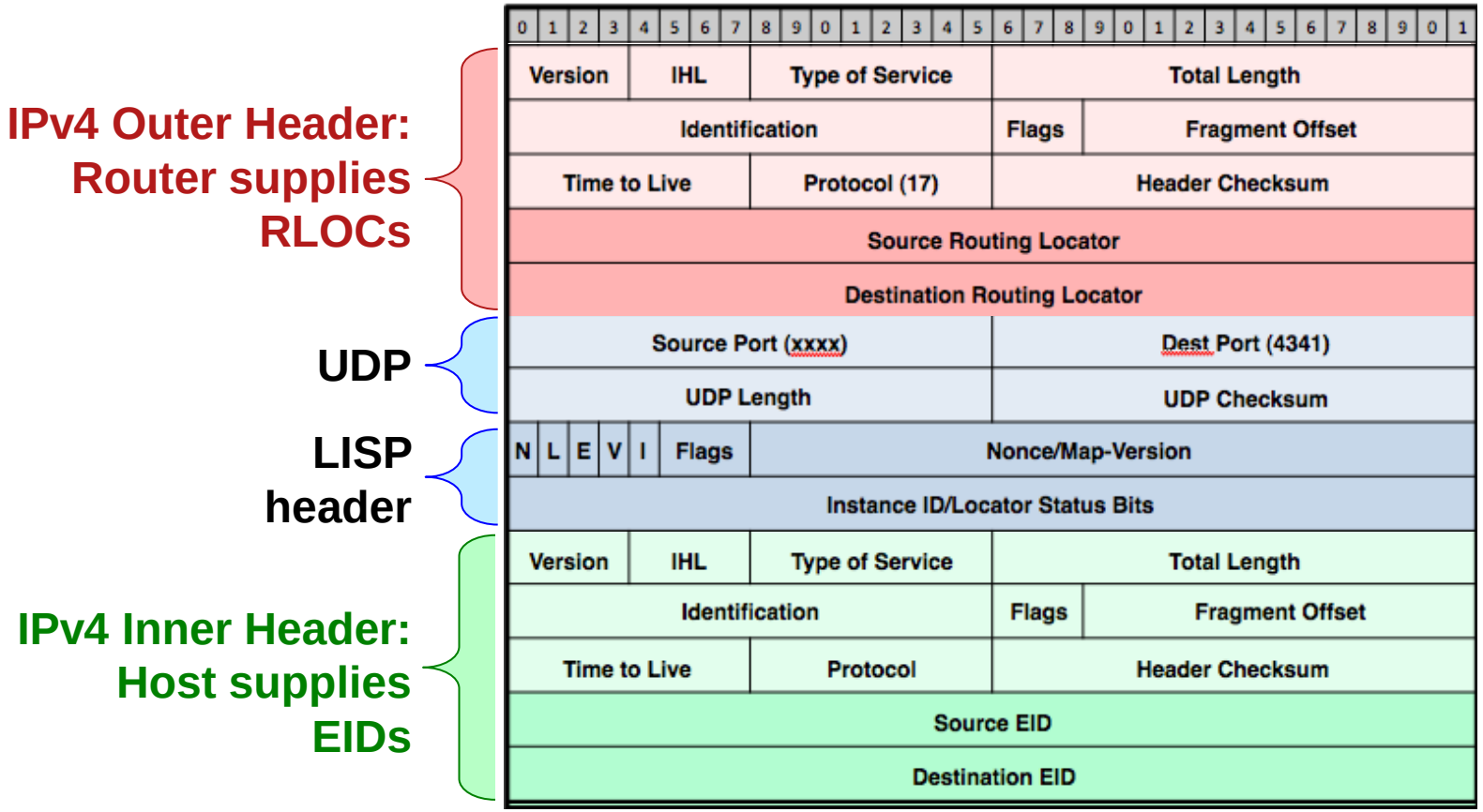
- LISP resolves **locators** for queried **identities**



LISP Operations

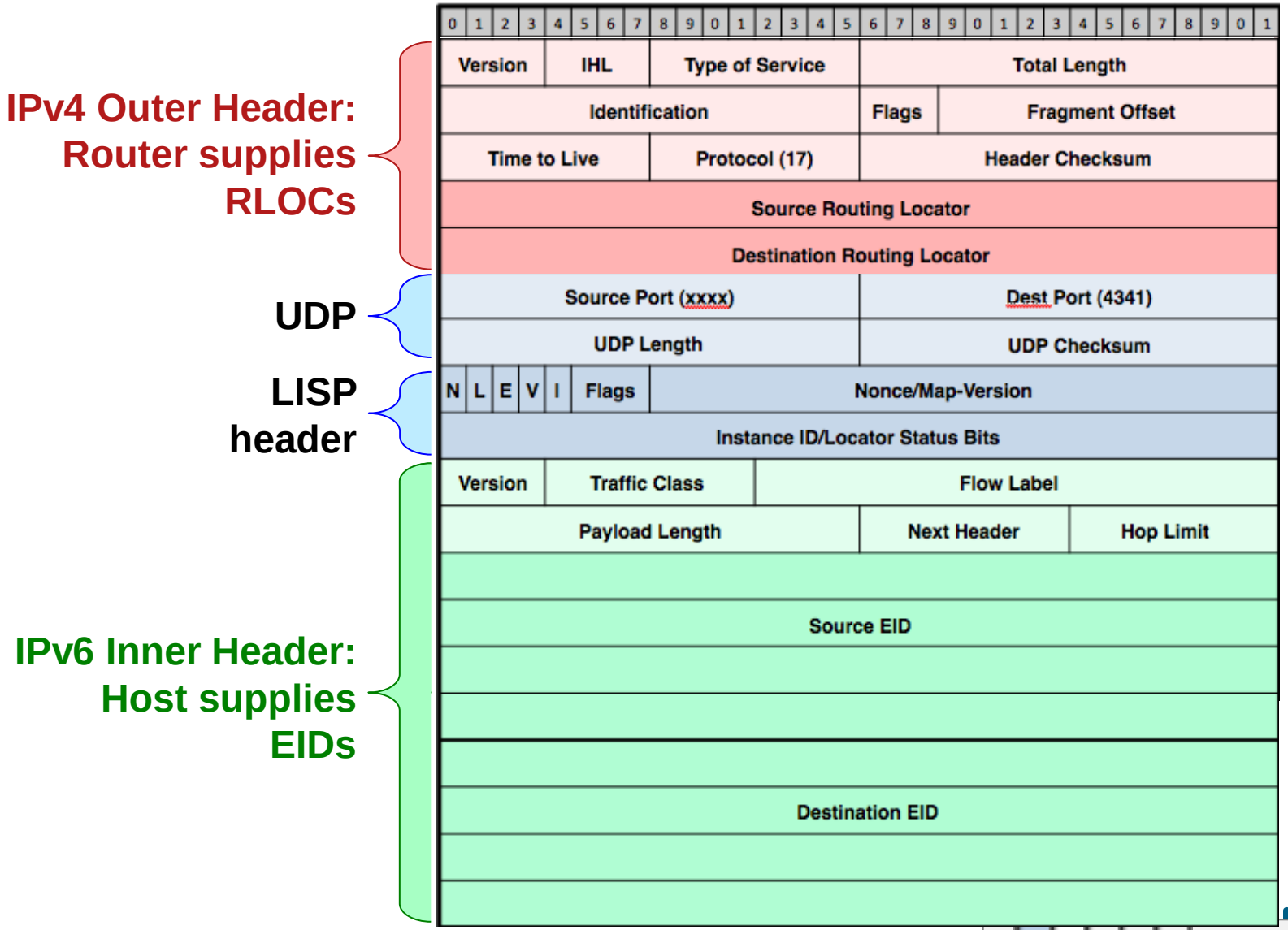
LISP – Data Header Format
IPv4 EID/IPv4 RLOC Example

draft-ietf-lisp-09



LISP – Data Header Format
IPv6 EID/IPv4 RLOC Example

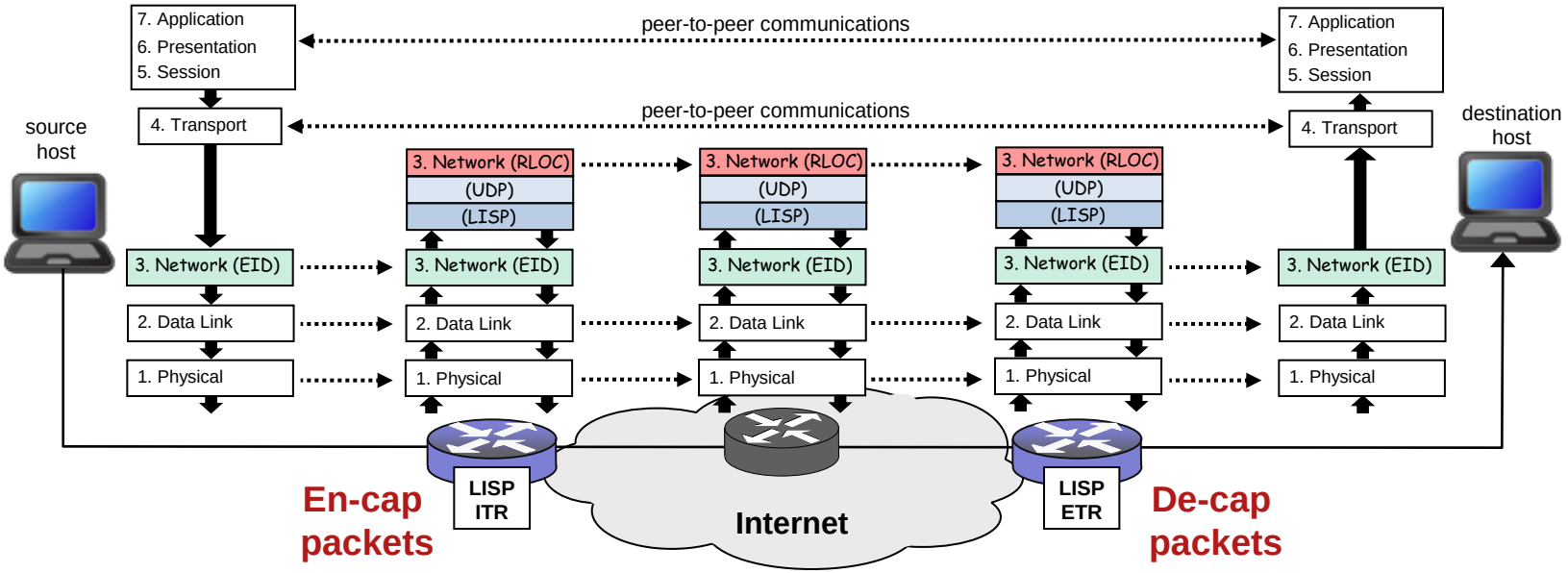
draft-ietf-lisp-09



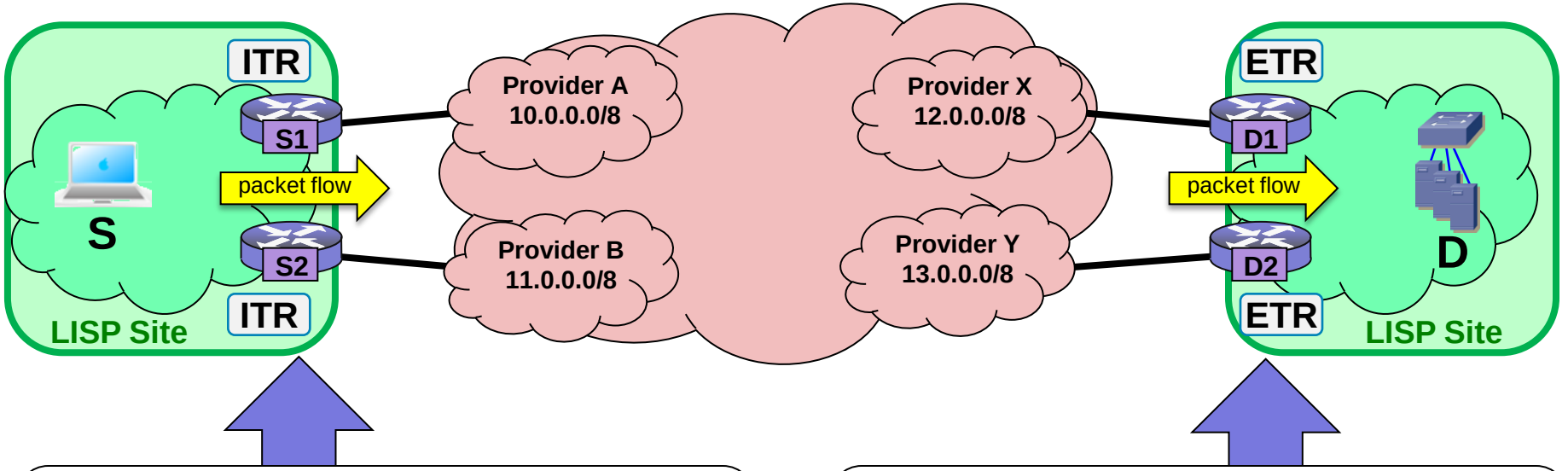
LISP – Data Plane Operations
End-to-End connection is between EIDs

Network-Based “map and encap” approach

- Requires the fewest changes to existing systems – only the CPE
- No changes in hosts, DNS, or core infrastructure
- New Mapping Services required for EID-to-RLOC mapping resolution



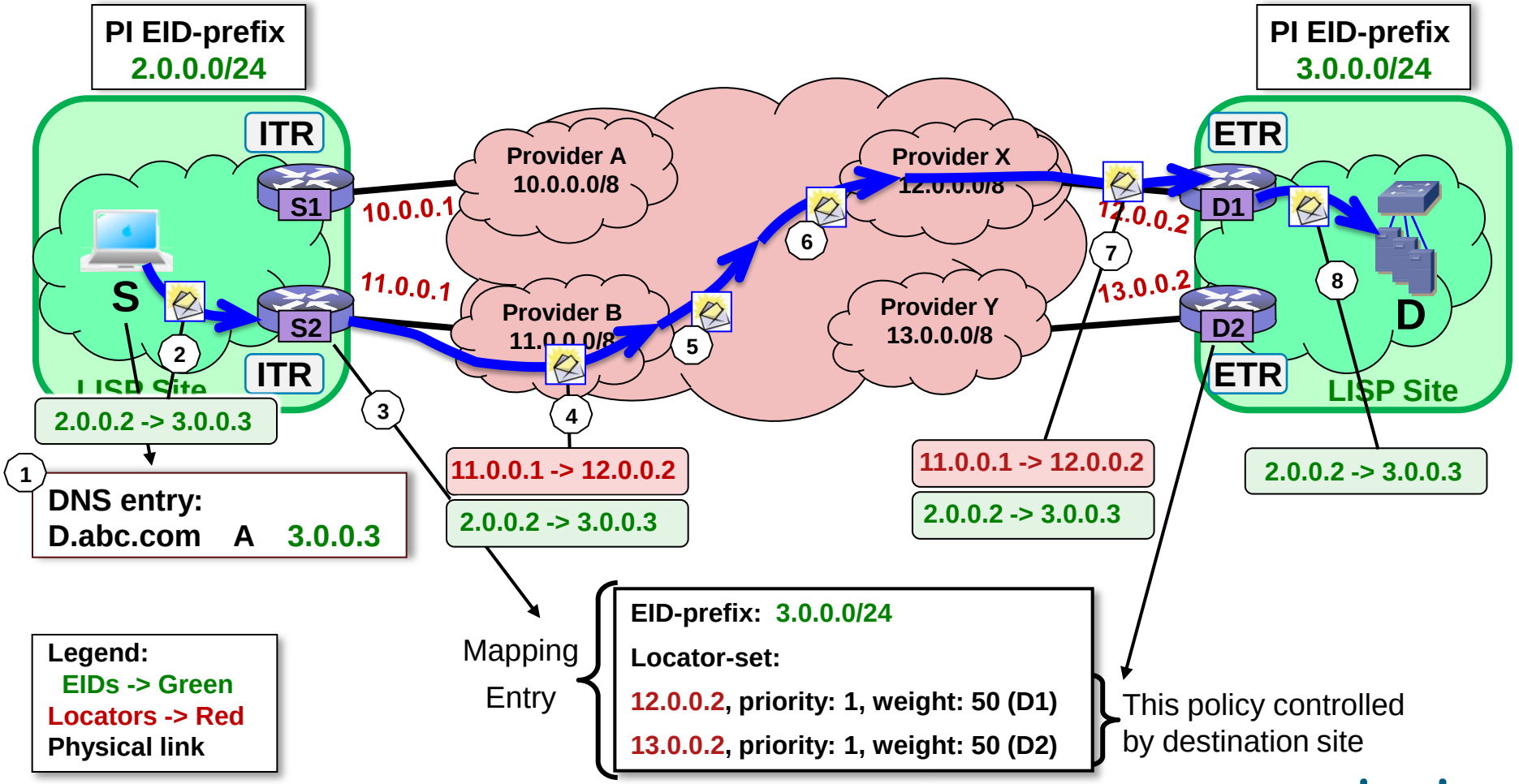
LISP Data Plane
Ingress/Egress Tunnel Router (xTR)



ITR – Ingress Tunnel Router
- Receives packets from site-facing interfaces
- Encapsulates to remote LISP site (or natively forwards to non-LISP site)

ETR – Egress Tunnel Router
- Receives packets from core-facing interfaces
- De-caps and delivers packets to local **EIDs** at the site

LISP Data Plane
Unicast Packet Forwarding



LISP Control Plane
Control Plane Messages

Control Plane **EID**Registration

Map-Register messages

Sent by ETR to Map-Server to register its associated **EID**prefixes

Specifies the **RLOC(s)**to be used by the Map-Server when forwarding Map-Requests to the ETR

Control Plane “Data-triggered” mapping service

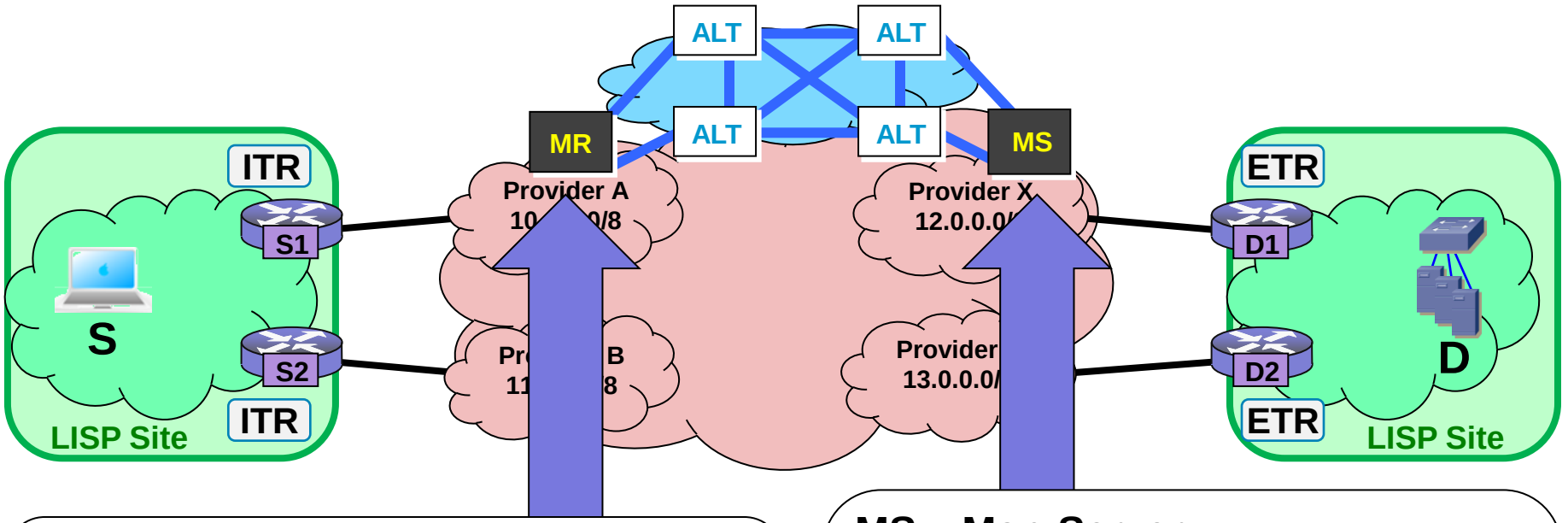
Map-Request messages

Sent by an ITR when it needsfor **EID**/**RLOC**mapping, to test an **RLOC**for reachability, or to refresh a mapping before TTL expiration

Map-Reply messages

Sent by an ETR in response to a valid map-request to provide the **EID**/**RLOC**mapping and site ingress Policy for the requested **EID**

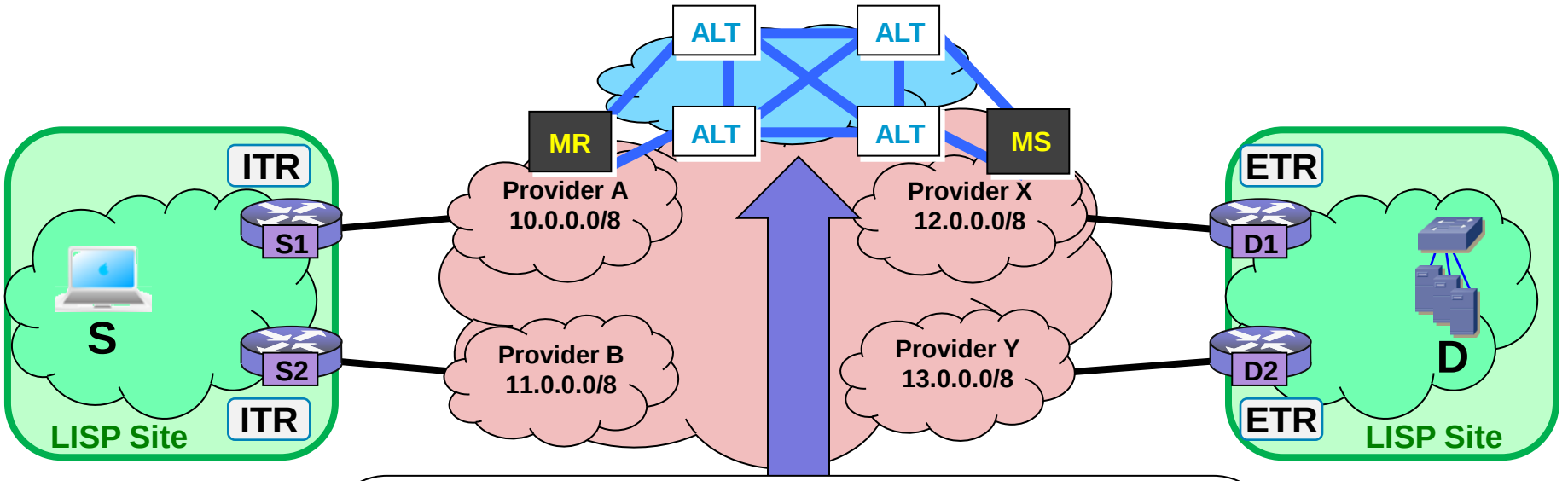
LISP Control Plane
Map-Server/Map-Resolver (MS/MR)



MR – Map-Resolver
- ReceivesMap-Requestfrom ITR.
- Forwards Map-Request onto the ALT topology.
- Sends Negative Map-Replies in response to Map-Requests for non-LISP sites.

MS – Map-Server
- LISP site ETRs Register their EID prefixes here; requires configured “lisp site” policy, authentication key.
- Injects routes for registered site EID prefixes into BGP ALT topology.
- Receives Map-Requests via ALT and forwards them to registered ETRs.

LISP Control Plane
LISP-ALT



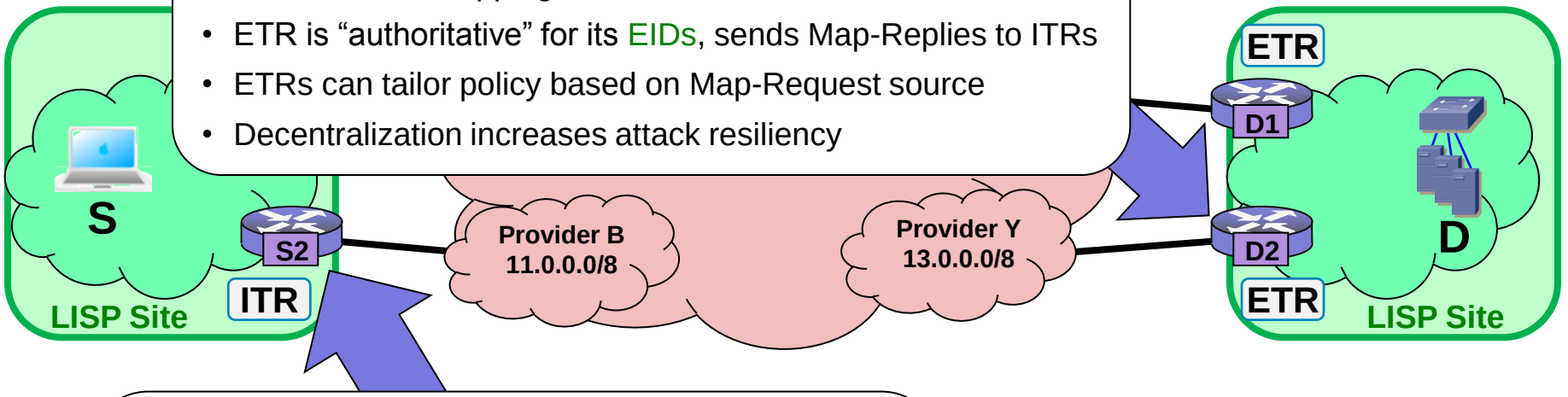
ALT – Alternate Topology

- Aggregate registered EID-prefixes along allocation hierarchy
- Advertises (pushes) EID-prefixes in Alternate BGP topology over GRE tunnels
- Map-Requests with EID destination address are forwarded over GRE topology.
- ALT peering connections and can be off-the-shelf gear, a router, commodity Linux host, etc.

LISP Control Plane
Mapping Database (ETR), Map-Cache (ITR)

LISP Site Mapping-Database

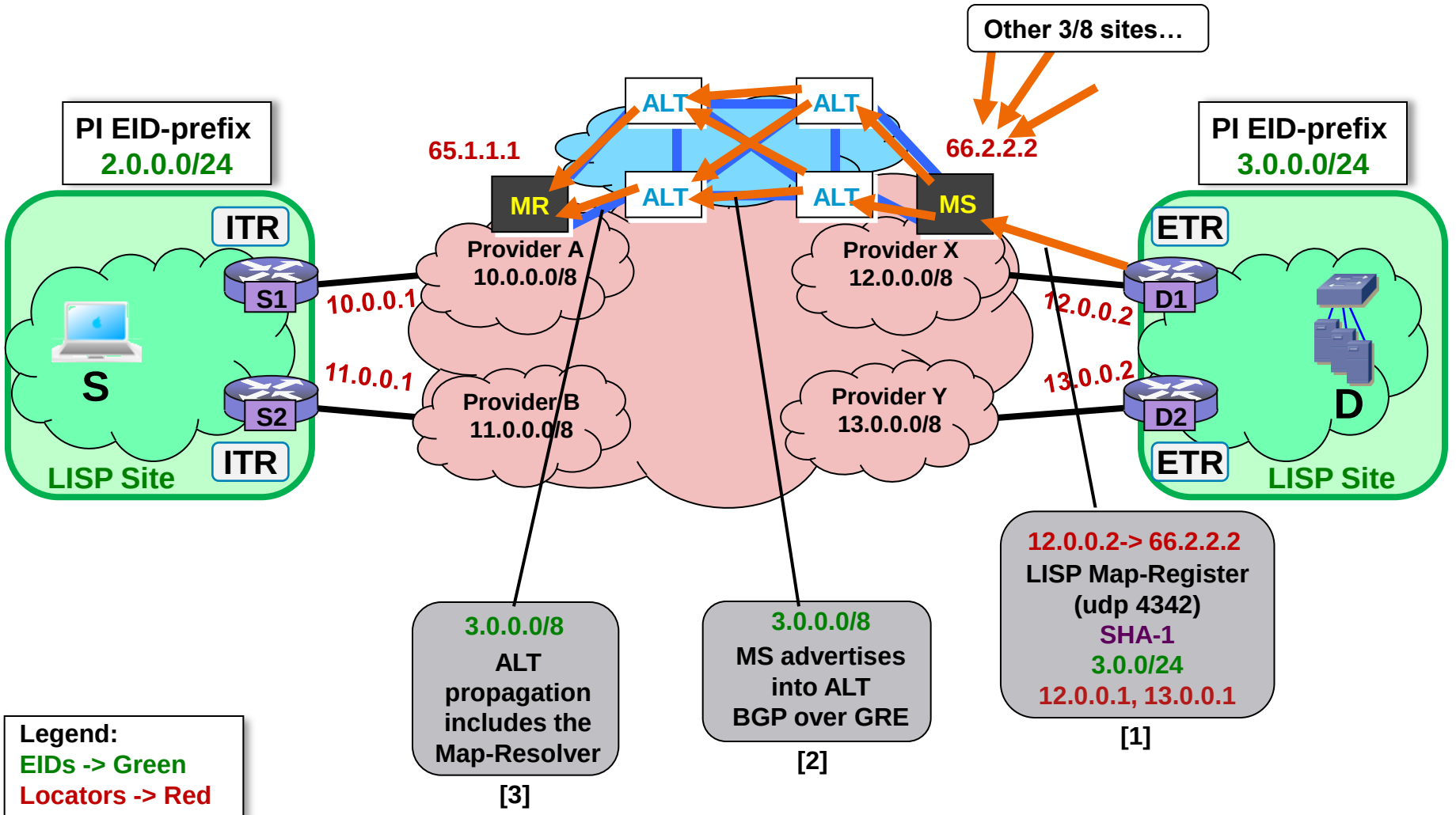
- EID-to-RLOC mappings in all ETRs for local LISP site
- ETR is “authoritative” for its EIDs, sends Map-Replies to ITRs
- ETRs can tailor policy based on Map-Request source
- Decentralization increases attack resiliency



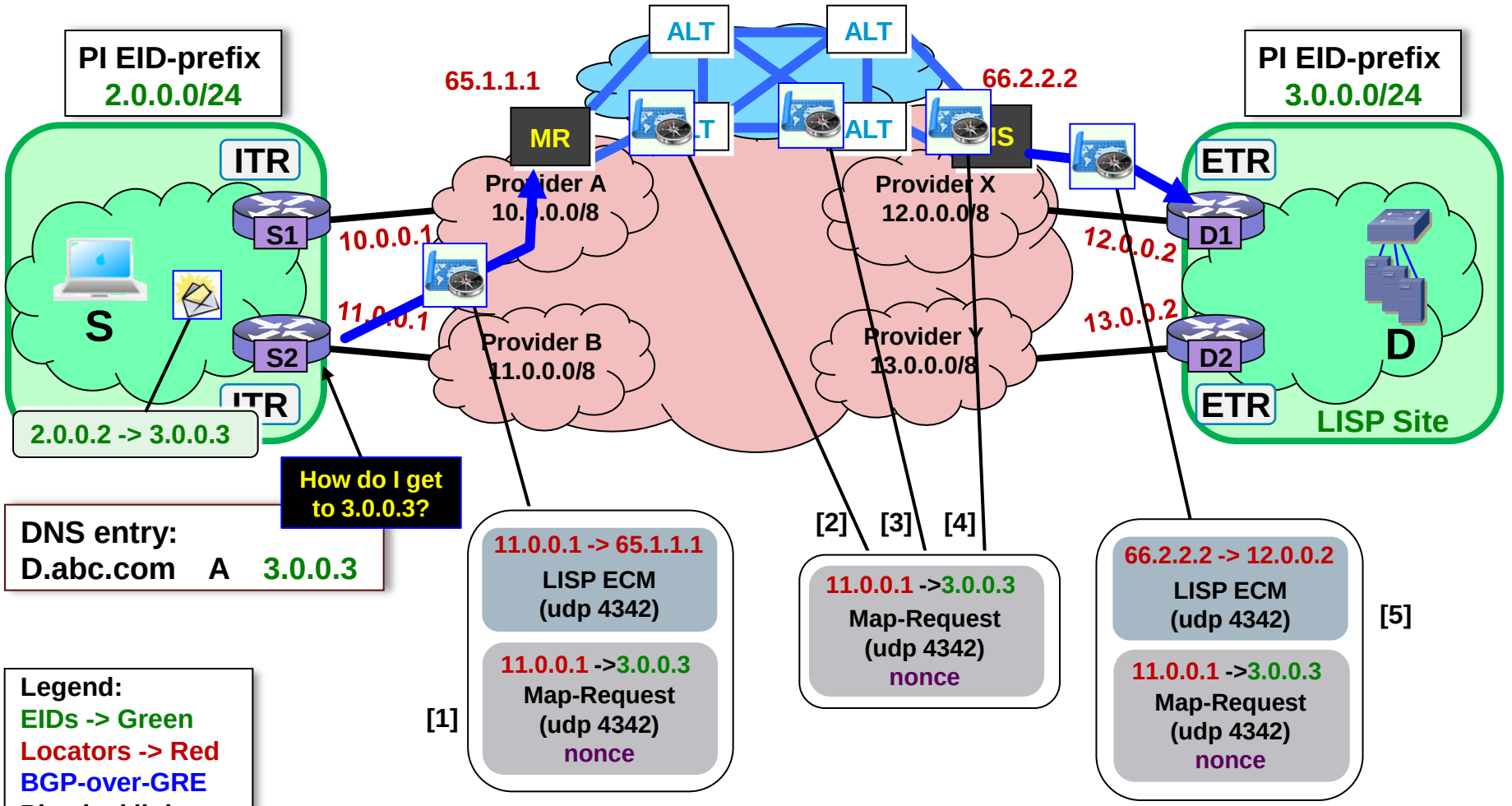
LISP Map Cache

- “Lives” on ITRs and only stores mappings for sites to which ITR is currently sending packets.
- Map-Cache populated by sending Map-Requests through ALT and receiving Map-Replies from ETRs
- ITRsmust respect Map-Reply policy, including TTLs, RLOC up/down status, RLOC priorities/weights

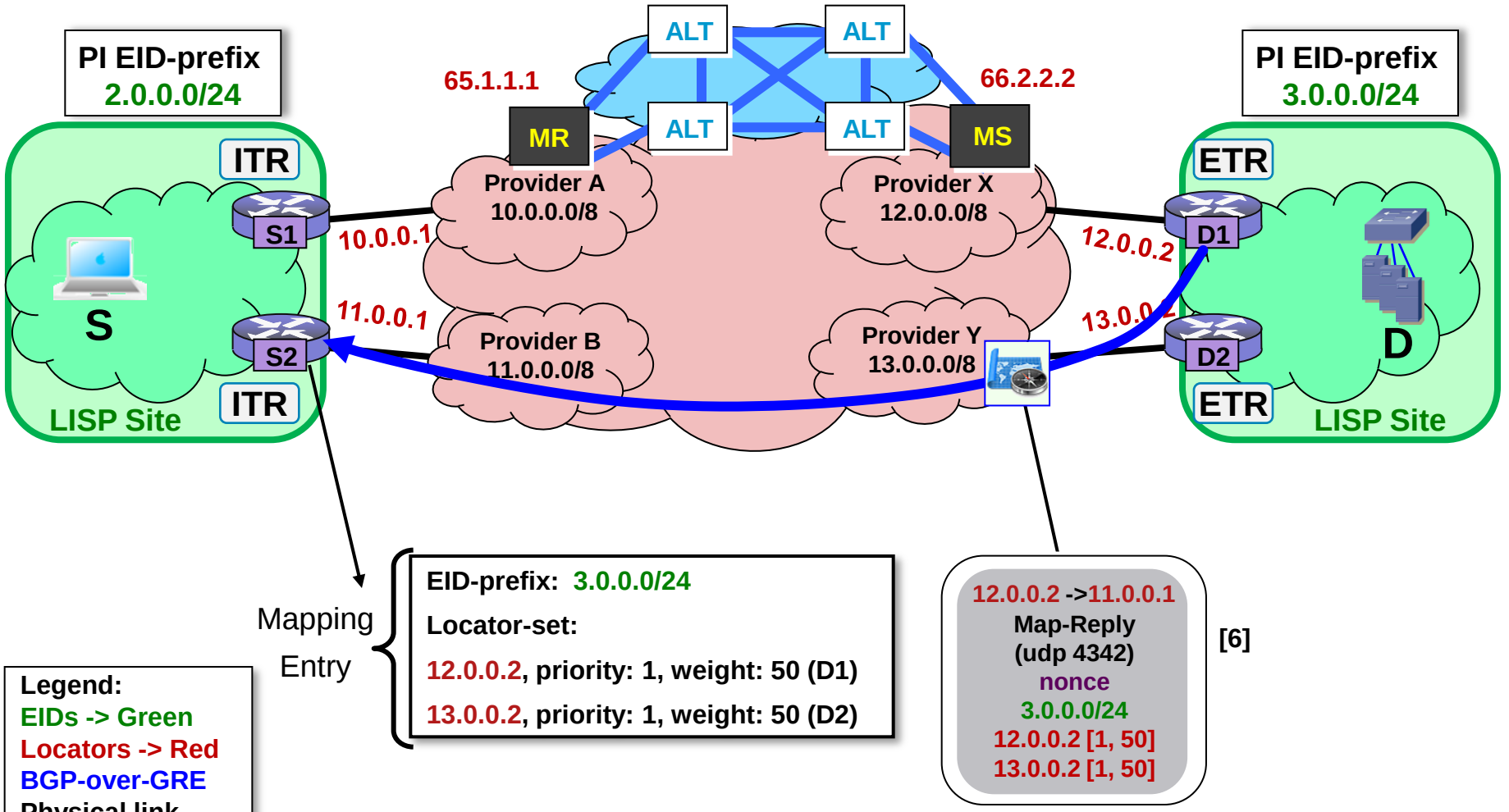
LISP Control Plane
Map-Registration example



LISP Control Plane
Map-Request example



LISP Control Plane
Map-Reply example



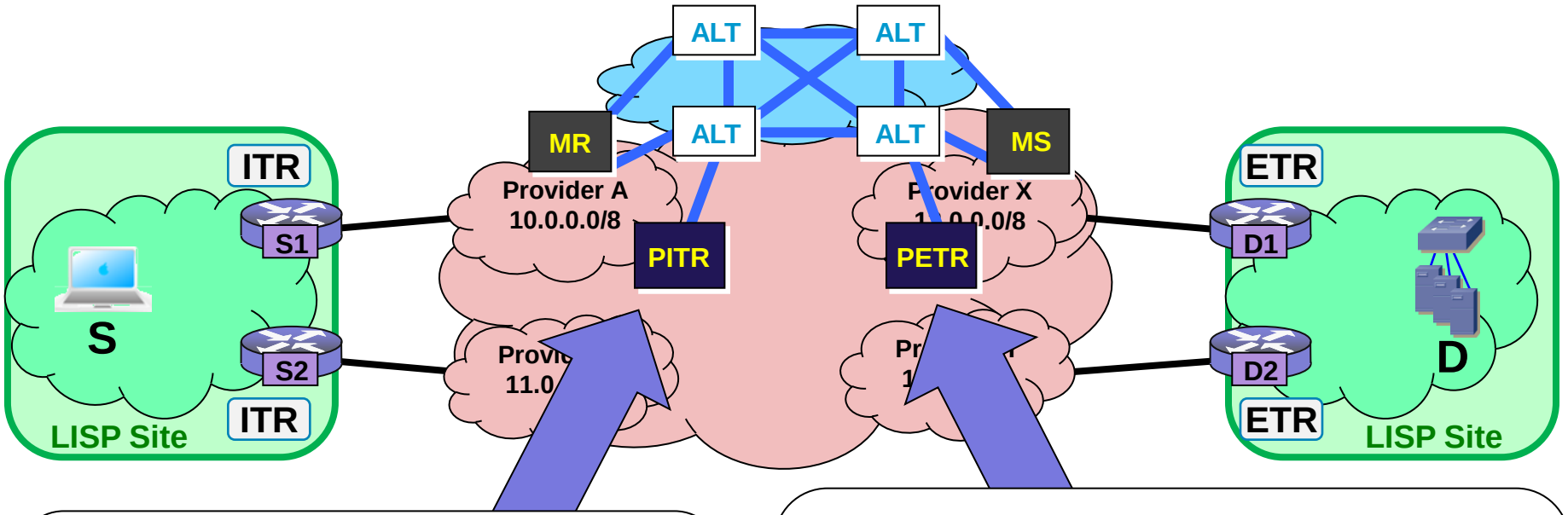
LISP Interworking
Day-One incremental deployment

- Early Recognition:
  - LISP will not be widely deployed day-one
  - Up-front recognition of an incremental deployment plan
- Interworking for:
  - **LISP-sites**to **non-LISP sites**(i.e. the rest of the Internet)
  - **non-LISP sites**to **LISP-sites**
- Two basic Techniques
  - Proxy ITR (PITR) and Proxy ETR (PETR)
  - LISP Network Address Translators (LISP-NAT)
- Proxy-ITR/Proxy-ETR are being deployed today

  Infrastructure LISP network entity

  Creates a monetized service opportunity for infrastructure players

LISP Interworking
Proxy Ingress/Egress Tunnel Routers (PITR/PETR)



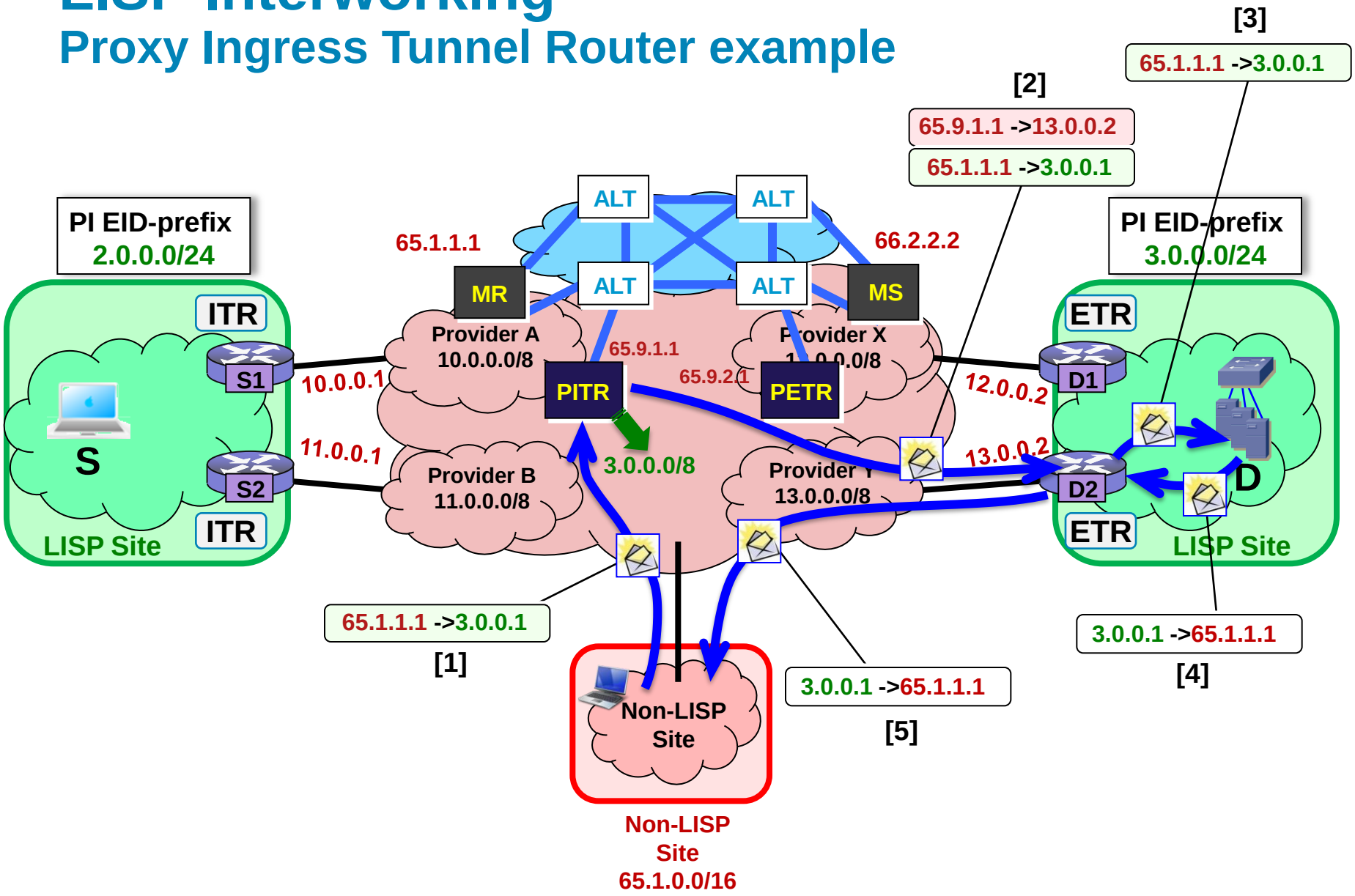
PITR – Proxy ITR

- Receives traffic from **non-LISP**sites; encapsulates traffic to **LISP sites**
- Advertises coarse-aggregate **EID** prefixes
- **LISP sites** see ingress TE “day-one”

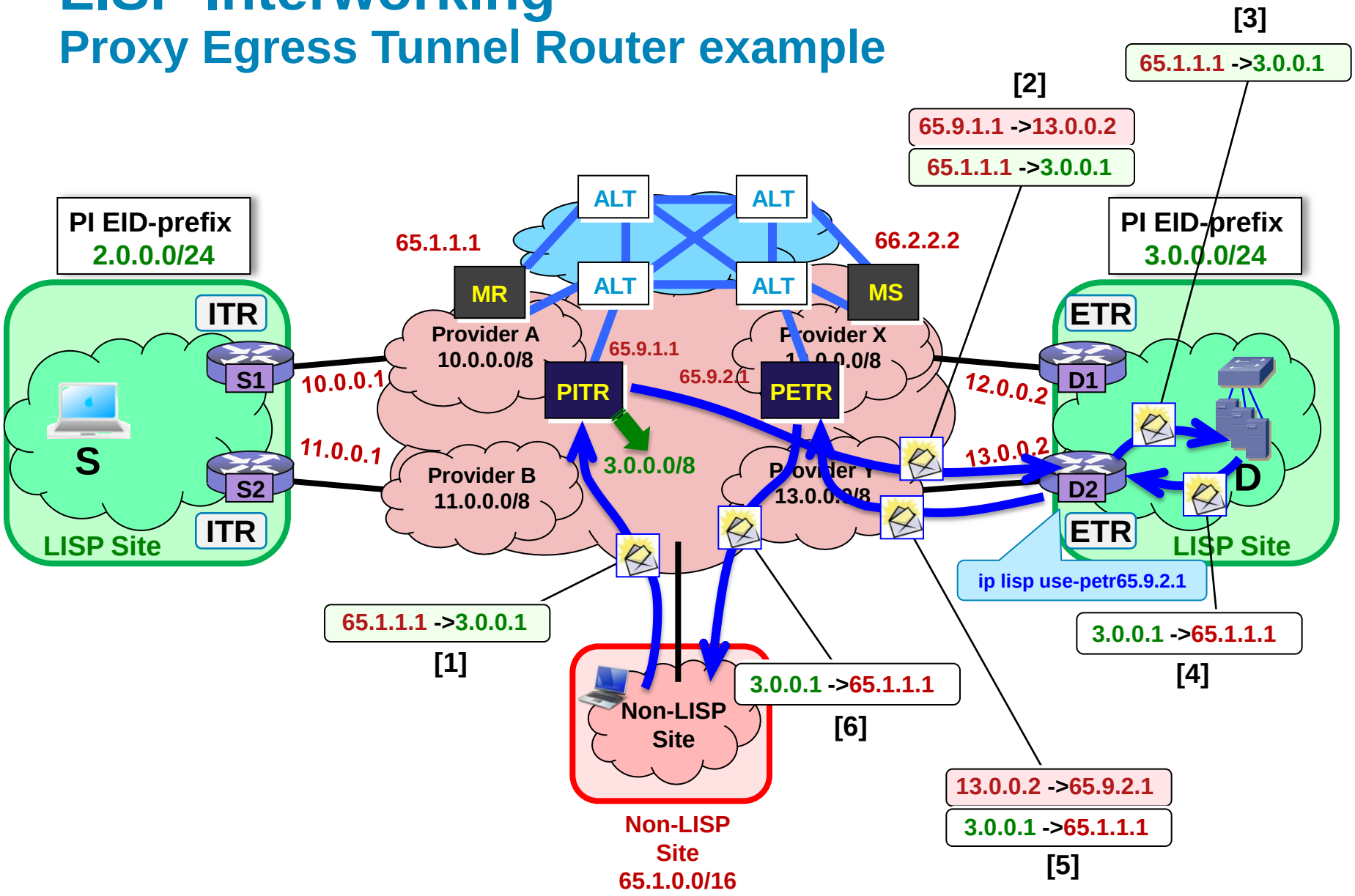
PETR – Proxy ETR

- Allows **IPv6 LISP**sites with **IPv4 RLOCs** to reach **IPv6 LISP**sites that only have **IPv6 RLOCs**
- Allows **LISP**sites with uRPF restrictions to reach **non-LISP**sites

LISP Interworking
Proxy Ingress Tunnel Router example



LISP Interworking
Proxy Egress Tunnel Router example



LISP and Security
Aspects of LISP Security

Security…

… of the protocol

- Inherent security of the protocol itself

… impact of the protocol on existing networks

- 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

LISP and Security
Security… of the protocol

Security… of the protocol

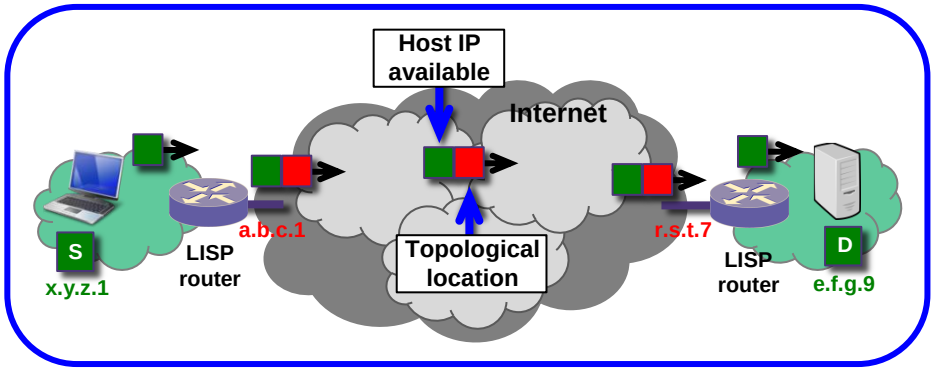
- Internet + LISP is no less secure than existing Internet
  - The protocol must be “deployable”
- Security of the protocol is added as driven by operational requirements
  - Authentication of Map-Registers
  - Nonce in Map-Request/Map-Reply
  - Other internal specifications (see Internet draft)
- Protocol developed to be enhanced by other security mechanisms as needed: e.g.
  - IPsec and Group Encrypted Transport (GET)
  - PKI for control plane

LISP and Security
Security… impact of protocol on existing networks

Security… impact of protocol on existing network

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

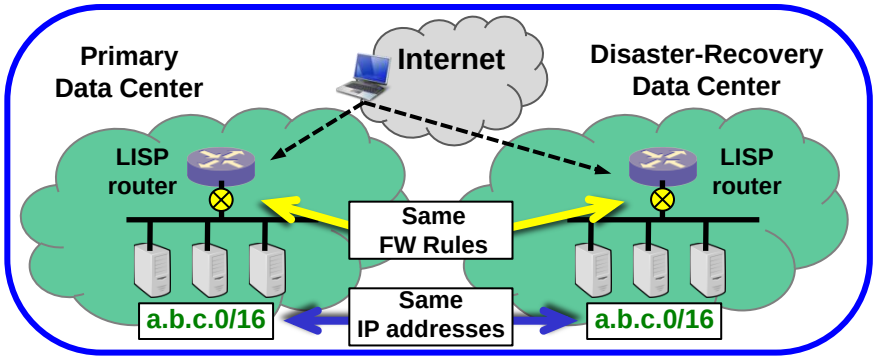


LISP and Security
Security… impact of protocol on existing networks

Security… impact of protocol on existing network

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



LISP and Security
Security… enabled by the protocol

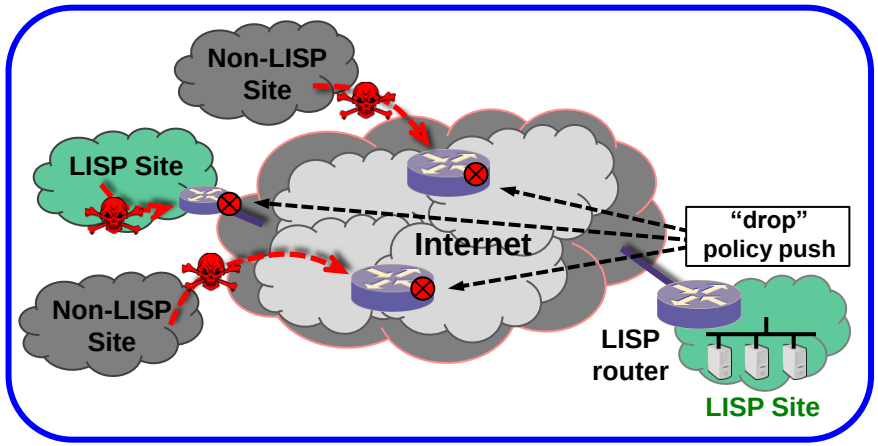
Security… enabled by the protocol

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 (ITR or PITR)
  - Simple “redirection” to scrubber center



LISP and Security
Security… enabled by the protocol

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