Comparison of Customer Edge Switching with LISP

Customer Edge Switching is presented in [1, 2, 4, 5] and LISP in [3].

The pronounced justification for the Locator/ID Split Protocol [3] is solving the problem of the scalability of the core while providing multi-homing to corporate networks without BGP (and at lower cost). Without introducing a trust model of any kind LISP proposes to introduce ingress and egress tunnel routers into a similar place where we place the trust boundaries. For the delivery of the first packets of a flow, LISP proposes several solutions, for example, to build a global signaling network called “an alternative topology” that can use EIDs for packet delivery. We immediately note that LISP does not deliver what the name of the protocol promises, i.e. it does not separate identifiers from routing addresses. It just has just two levels of addresses. Both EIDs and routing locators (RLOCs) in LISP are globally unique 32-bit addresses in case IPv4 is used for forwarding. Since we already have around 1.8 billion users on the net, we argue that introducing a 32-bit globally unique ID does not scale to even the present needs, not to talk about the future needs. LISP advocates that its purpose should be reached using routing only. We argue that we should use a combination of routing and directory services, the latter for example based on DNS. Table 1 compares, LISP as a protocol with CES (a solution) using multiple criteria. The purpose is to show what else, besides a protocol is needed to solve current problems.

Table 1: Comparison of LISP [3] and Customer Edge Switching

Criteria	LISP	CES with CE Traversal Protocol
Purpose	Scaling the Internet core Provision of multi-homing without BGP	Trust processing for customers with side effect of scaling the core and multi-homing of customer networks.
Scaling to users	EID is a 32 bit globally unique ID/address → provides only marginal help with address exhaustion in IPv4	Solves the problem of IPv4 address exhaustion by address reuse.
Scaling to short flows	Poor	As good as NATs
Scaling to connection arrivals	Based on router capacity and EID/RLOC mapping system capacity	Base solution for legacy interworking scales to low level of arrivals to servers behind a CES, i.e to many types of IoT objects and to mobile handset hosted servers. CES to CES connection arrivals limited only by CES capacity. Scalability is improved by protocol proxies e.g. for http.
Unwanted traffic	Not addressed (seen as a separate problem)	Trust processing of incoming traffic by Trust Function/Policy Engine. Open to extensions for proactive actions against unwanted traffic.
Additional problems solved		(1)Hiding customer networks from the core and the core from the customer networks (2) Provides interrupt driven access for mobile devices
Private addressing in customer networks	Not addressed, seen as an independent issue, EIDs are revealed to correspondent hosts	Assumes private addressing of hosts. Private addresses are not revealed to outsiders making network scanning harder
Trust	Not addressed	CES has a fully blown policy for managing trust and protecting the users it serves. CES and CETP are building blocks for an Internet wide Trust Framework.
Signaling	Proposes a separate signaling network for probes and map-requests.	No separate signaling network, no explicit signaling for setting up state in CES. Crossing

	Uses explicit signaling for setting up state in Tunnel Routers	multi-homed trust borders seen as an on-demand routing problem. Additional control of setting up and managing connection state is supported by CETP signaling (many TLVs)
Interworking with legacy hosts	LISP tries to be invisible to hosts	CES is a like a Firewall, it uses ALG to process protocols that use IP addresses as IDs. For well designed protocols CES is invisible like a router.
Use of DNS	Not addressed	Relies on DNS for name to ID server mapping and local ID servers for ID to address mapping
IPv6	Assumes IPv6 for solving the address exhaustion problem. De-facto not needed in the core network.	Use of IPv4 or IPv6 is seen as independent of collaborative firewalling. However, we expect that IPv6 is not needed in the near future or demand for it is very limited.
Nature of Identity	ID is an IP address	Several types of Identities can be supported by the tunneling protocol e.g.: + Identity is a Random value that is unique with high probability in a CES or + a deterministic 32 bit value allocated by operators of an ID DHCP service or + an ID assured by operators or + ID is certified by a CA + ID identifies an object in IoT. ID is the key to packet admission and carries no addressing/locating semantics.
Locators	IPv4 addresses	IPv4 addresses, NSAP –like MAC addresses in a Carrier Grade Ethernet transport network etc. CETP is independent of RLOC types
Traffic Engineering and OAM	Point solutions are integrated in LISP	Can rely on Carrier Grade packet transport including e.g. Y.1731 for OAM. RLOC and flow hot swaps are supported by CETP
Changes in hosts	None	None mandatory
Security	Vulnerable to many attacks	Secure (to be proven…)
Deployment	ALT signaling network needed. Benefits require that both ends have invested in Tunnel Routers	Benefits require that at least one end has invested in Customer Edge Switches. Full benefits require both ingress and egress CES.
Business case	High cost to operators for implementing the service of EID to RLOC mapping. Weak reasons for corporations to invest.	Mobile operators can sell new services to customers. Corporations can better protect their servers and hosts from attacks

A variant of LISP (called LISP 2) that to an extent relied on DNS was discussed earlier but abandoned because it is “not pure that the directory is dependent on routing and routing on directory” [3]. We argue that instead of creating a global signaling network for delivering the first packets of each new flow to a new egress node or any other global service for EID to RLOC mapping, it is more cost efficient and technically more pure to store the routing locators of an egress trust domain in a directory like DNS and determine which one of them to use dynamically based on an on-demand edge-to-edge protocol. From the experience of Internet routing we know that it is not a good idea to let a stub network advertise its addresses using a dynamic routing protocol to the public network. Rather it is simpler to use static routing information with some dynamic supervision of the links on the interface or even reachability of the address block of the stub network. With this experience in mind, we suggest storing the routing locators of an egress trust domain in DNS or a similar directory and establishing which one of the RLOCs to use dynamically. This process of dynamic selection of the current RLOC can be seen as dynamic on-demand routing across the trust boundary. It is sufficient that the DNS stores just the default preferences of the RLOCs while the tunneling protocol/edge traversal protocol takes care of the dynamic changes in the preferences.

To summarize, we argue that Customer Edge Switching is a high value, easy to deploy proposition to both operators and customers while we do not see good reasons to invest in LISP. It is however possible to use LISP as an on-demand edge routing protocol without the global "alternative topology" as part of our solution (with less functionality than CETP). LISP introduces point solutions for Traffic Engineering and OAM. We argue that a comprehensive OAM framework, specified in Y.1731 exists and that in order to reduce the cost of provisioning mission critical packet transport an OAM framework is needed rather than yet another point solution. Moreover, traffic engineering is an inherent feature of a Carrier Grade packet transport system. Once again, we argue that let's go for the real thing rather than for another point solution that will be costly to manage for the operators.

Note: As of March-2012, CES and CETP are research prototypes with core functions verified and ongoing work progressing on the rest of the functionality.

References

[1] Kantola, R., Implementing Trust-to-Trust with Customer Edge Switching, in press for AMCA in connection with AINA 2010.

[2] L. Virtanen, Communicating Globally Using Private IP Addresses, M.Sc thesis, Comnet/TKK, 2009.

[3] D. Farinacci, V. Fuller, et.al, Locator/ID Separation Protocol (LISP), draft-ietf-lisp-06.txt, Jan 25, 2010 (see newer versions…).

[4] Raimo Kantola, www.re2ee.org, Protocols.

[5] Raimo Kantola, M. Luoma, J. Manner, Future Internet is by Ethernet, IFIP Network of the Future, in press, Sep-2010, Brisbane.