University of Würzburg
Institute of Computer Science
Research Report Series

Global Locator, Local Locator, and Identifier Split (GLI-Split)

Michael Menth[1], Matthias Hartmann[1], Dominik Klein[1]

Report No. 470 April 2010

[1] University of Würzburg
Institute of Computer Science
Chair of Distributed Systems
Würzburg, Germany
Email:
{menth,hartmann,dominik.klein}@informatik.uni-wuerzburg.de

An updated version of this technical report has been published in the MDPI Future Internet open access journal. The document is available via https://www.mdpi.com/1999-5903/5/1/67.

Global Locator, Local Locator, and Identifier Split (GLI-Split)

Michael Menth, Matthias Hartmann, Dominik Klein
University of Würzburg, Institute of Computer Science
Am Hubland, D-97074 Würzburg, Germany
Email: {menth,hartmann,dominik.klein}@informatik.uni-wuerzburg.de

Abstract—**GLI-Split is a new addressing and routing architecture for the Internet. It splits the functionality of current IP addresses into a global locator, a local locator, and an identifier, and encodes them in IPv6 addresses. It implements the locator/identifier split and makes routing in the core of the Internet more scalable. GLI-Split can be incrementally deployed and it is backward-compatible with the IPv6 Internet. It provides more flexibility for edge networks than the addressing and routing architecture of today's Internet and creates thereby important incentives for early adopters. GLI-Split requires upgraded networking stacks in hosts, but non-upgraded hosts can also be accommodated in GLI-domains and benefit from a reduced set of advantages.**

I. INTRODUCTION

Typical BGP routing tables in the default-free zone (DFZ) of the Internet nowadays hold about 300,000 entries and grow faster and faster [1]. This has been recognized as a potential threat for the Internet's scalability in the future [2]. The expansion of the current IPv4 Internet is at its limits as the pool of free IPv4 addresses will be exhausted in about two years [3]. We believe that this will lead to increased IPv6 deployment. IPv6 has room for a multitude of addresses and possibly causes almost unrestricted growth of the routing table sizes in the DFZ. Hence, at least for the IPv6 Internet a new and more scalable routing architecture is required. Separating current IP addresses into two independent pieces of reachability and identification information helps to reduce this growth and is called locator/identifier split (Loc/ID split) [4]. The stable identifier (ID) gives a global name to a node. A changeable locator (Loc) describes how the node can currently be reached through the global Internet. Furthermore, a mapping system (MS) is needed to map locators to identifiers. This principle makes routing in the stable Internet core more scalable because core routing is not affected by changed attachment points and multihoming of edge networks. The deployment of Loc/ID split in the Internet requires modifications to the current routing and addressing architecture. Its development takes a long time and implies hard- and software upgrades. Therefore, the modified Internet architecture should also satisfy additional requirements like support for renumbering, multi-homing, multipath transmission, security, and others [5], [6].

Most of the current proposals for a future routing and addressing architecture [7]–[13] implement a kind of Loc/ID split. They essentially separate core and edge routing, but local routing is still performed on IDs. When nodes change their position within a local routing domain or move from one edge network to another, they either require a new ID or the local routing system must account for that change. Replacing a node's ID breaks the function of an ID and adapting the local routing system makes routing more complex. A few proposals implement a true Loc/ID split [14]–[17], but they take a clean-slate approach, i.e., they are not backward-compatible with today's Internet which makes them hard to deploy.

This work proposes GLI-Split as a new concept for future Internet routing and addressing. It splits the functionality of IP addresses into global locators, local locators, and identifiers and implements a true Loc/ID split with IDs that are independent from the current location. IDs and locators are encoded in regular IPv6 addresses so that no new routing protocols are required. GLI-Split is backward-compatible with the IPv6 Internet and interworking is simple. Individual networks can be upgraded to GLI-Split without any impact on communication with other domains. GLI-Split facilitates provider changes, renumbering, multi-homing, multipath-routing, traffic engineering, and provides improved mobility support. To take advantage of all these benefits, nodes in GLI-domains require upgraded networking stacks, but nodes without upgraded networking stacks can also be accommodated in GLI-domains and enjoy benefits. This is important for incremental deployability. We do not consider interworking solutions between GLI-Split and the IPv4 Internet as GLI-Split is compatible with IPv6 and interworking solutions between IPv4 and IPv6 already exist.

The paper is structured as follows. Section II presents fundamentals of GLI-Split, Section III and Section IV explain how GLI-Split works with upgraded and non-upgraded nodes. We summarize the benefits of GLI-Split in Section V, discuss related work in Section VI, and give conclusions in Section VII.

II. FUNDAMENTALS OF GLI-SPLIT

This section introduces some basic nomenclature, shows the structure of GLI-addresses, and explains their relation to DNS.

This work is funded by Deutsche Forschungsgemeinschaft (DFG) under grant TR257/23-2. The authors alone are responsible for the content of the paper.

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

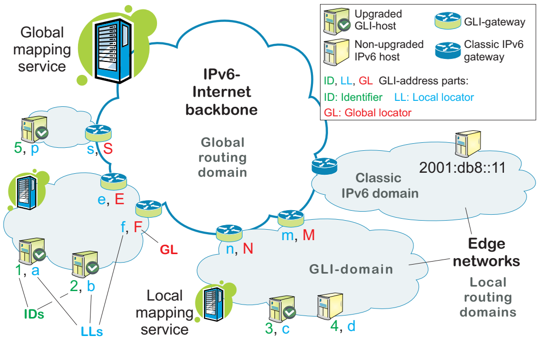

Fig. 1. GLI-nodes and GLI-gateways have an identifier (ID) for identification and a local locator (LL) for routing in edge networks; in addition, GLI-gateways have a global locator (GL) which is used for routing in the IPv6 backbone.

A. General Idea and Nomenclature

Edge networks like those of companies may implement GLI-Split. We call them GLI-domains while we call others *classic IPv6* domains. Nodes of a GLI-domain are GLI-nodes and its border routers are GLI-gateways. GLI-nodes with a special GLI-(networking-)stack are called *upgraded* while others are called *classic IPv6* nodes. GLI-nodes and GLI-gateways are identified by a globally unique identifier (ID). They have a local locator (LL) that describes their position within their GLI-domain and serves for local routing. Furthermore, each GLI-gateway has a globally unique global locator (GL) that describes its position in the IPv6 backbone. A global mapping service (MS) maps IDs to GLs and a local MS maps IDs to LLs. This setting is illustrated in Figure 1. IDs are denoted by integral numbers, LLs by lowercase letters, and GLs by uppercase letters. In the examples of this paper, we refer to parts of the setting in this figure. We designate GLI-nodes by their IDs, i.e., node 1 is *the node with ID 1*.

B. GLI-Addresses

GLI-Split encodes ID and locator information in IPv6 addresses to be compatible with classic IPv6. The ID of a GLI-address is fixed, while the locator information can be replaced by GLI-hosts and -gateways on the path between source and destination. According to the current locator information, we distinguish three different types of addresses: identifier addresses, local addresses, and global addresses.

1) Format: Figure 2 shows the encoding of the three address types reusing the 128-bit IPv6 address format. The 64 higher-order bits are used for routing and special tasks, while the 64 lower-order bits contain an identifier. All GLI-addresses have a special 8 bit GLI-prefix to differentiate them from other IPv6 addresses. Routing is based only on the higher-order bits and our assumption is that appropriate GLI-prefixes are announced in the IPv6 backbone. Identifier addresses have the locator field filled with padding zeroes. A marker (L, G) indicates whether the locator part contains a local or global locator. Global addresses have the GL followed by a GAP-bit which is used for multipath-routing, traffic engineering, and interworking. The remaining 16 bits are used for checksum compensation so that checksums calculated, e.g., by TCP, are still valid after locator changes. In classic IPv6, these address bits are used for local routing within a subnet. This functionality is not required in GLI-Split where local routing is performed by the LL.

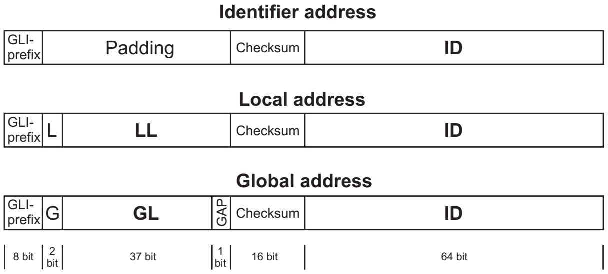

Fig. 2. Three types of GLI-addresses are encoded in an IPv6 address.

2) Use: An *identifier address* is an endpoint identifier independent of any locator information. It is used in the transport layer of upgraded GLI-nodes, e.g., as source or destination address in TCP sockets. A *local address* is used for forwarding within a GLI-domain. As the LL has only site-local meaning, a local address must never leave a GLI-domain. A *global address* is mainly used for routing outside GLI-domains. The GL belongs to a GLI-gateway of the host's GLI-domain and is allocated from the address space of the ISP that is connecting the GLI-domain to the Internet. Inside a GLI-domain, packets addressed to global addresses are usually forwarded to a default gateway. However, if the GL in the destination address belongs to a GLI-gateway of that GLI-domain, the packet is routed to that GLI-gateway.

3) Assignment: GLs are IPv6 prefixes that are globally assigned to GLI-gateways from ISPs in a hierarchical way, just like regular IPv6 prefixes are assigned today in the Internet. IDs are also hierarchically assigned in a similar way, but they are independent from any routing information. The hierarchy here is only important to improve the scalability of the MS, which can then work with ID-prefixes instead of individual IDs. HIP-like IDs may be also supported using the concept in [18]. LLs are locally allocated according to a network's topology and management needs. They can be dynamically changed and re-assigned to IDs when nodes move within a GLI-domain.

The assignment of LLs to nodes inside a GLI-domain may be done by enhanced DHCP. This DHCP also communicates the information how to reach the mapping service. An upgraded GLI-node knows its ID, tells it to the DHCP which returns a LL as well a set of GLs. The upgraded GLI-node registers the ID-to-LL and ID-to-GL mappings with the local and global MS including the information that the associated node has upgraded GLI-functionality. When an upgraded node changes its attachment point, it performs this procedure again.For non-upgraded nodes in GLI-domains, the assignment process works differently. The DHCP server knows

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

by configuration the MAC address and the ID for every non-upgraded node in its area and assigns a local GLI-address to this node reflecting the ID of the node. Due to missing capabilities of non-upgraded nodes, the DHCP server is in charge of registering the appropriate ID-to-LL and ID-to-GL mapping with the local and global MS.

4) Notation: In our examples, local addresses are written as a combination of the LL (a lower case character) and the ID (an integer number). Example: '$a.1$'. Global addresses are written as a combination of the GL (an upper case character) and the ID. Example: '$E.1$'. The activated GAP-bit is denoted by a (g) after the GL. Example: '$E(g).1$'. Identifier addresses are denoted only by their IDs. Example: '.1'.

C. Name Resolution

To start a communication session, the initiating host resolves a DNS name (e.g. host3.other-glidomain.net) into an IP address. If the returned IP address is a GLI-address, GLI-nodes or GLI-gateways possibly require an additional lookup to the mapping service to find an appropriate LL or GL for the ID.

1) Use of the DNS: When a DNS name denotes a GLI-node, it returns a global GLI-address with a set GAP-bit. As this IPv6 address is globally routable, hosts outside of GLI-domains can use this address without any modifications.

2) Use of the Mapping Service: The mapping service (MS) consists of a local and a global component. The local MS stores a set of local GLI-addresses for IDs residing within its local GLI-domain while the global MS stores a set of global GLI-addresses for any ID. Sets of addresses are required when routing alternatives exist, e.g., inside a GLI-domain when the ID is connected to several networks in the same GLI-domain, or, in the global MS when the ID belongs to a GLI-node in a multi-homed domain.

GLI-hosts with upgraded networking stacks are able to recognize when an IP address returned from the DNS belongs to a GLI-node. In that case, they extract the ID from that address and query the local MS for an appropriate GLI-address. If the destination node resides in the same GLI-domain as the requesting node, the local MS returns a set of local GLI-addresses, otherwise it notifies the requesting node that the requested ID is not part of the same GLI-domain. Then, the GLI-node requests the global MS which returns a set of global GLI-addresses.

Like the DNS, the MS is queried only for the first occurrence of a new ID and the query result is locally cached for later use to avoid that the MS becomes a performance bottleneck [19]. We do not specify how the MS works in detail because many technical solutions have already been proposed for that purpose [20]–[23].

III. GLI-SPLIT WITH UPGRADED HOSTS

We describe the communication between two GLI-nodes with upgraded networking stacks and how networking details are hidden from the transport layer. We explain gateway selection and global address preservation which are needed for interworking with non-GLI-nodes, multipath support, and traffic engineering. Finally, we propose improved mobility features and address some security attacks including countermeasures.

A. Communication between Upgraded GLI-Nodes

We describe how GLI-node 1 establishes communication with another GLI-node with the DNS name hostX.domainY.net. GLI-node 1 queries the DNS and obtains an IPv6 address. As the prefix of the returned address indicates a GLI-address, GLI-node 1 extracts the ID from that address. We distinguish whether both GLI-nodes are in the same domain or in different domains.

1) Communication within a Single GLI-Domain: GLI-node 1 communicates with GLI-node 2 in the same GLI-domain (see Figure 1). Node 1 queries the local MS for a local GLI-address of ID 2. As both GLI-nodes are part of the same GLI-domain, the MS responds with one or several local GLI-addresses for node 2. Node 1 chooses one of them as destination address and its own local GLI-address as source address for communication with node 2.

2) Communication between Different GLI-Domains: GLI-node 1 communicates with GLI-node 3 in a different GLI-domain (see Figure 1). When node 1 queries the local MS for local GLI-addresses of ID 3, it receives a negative answer. Then, node 1 queries the global MS for a global GLI-address of ID 3. Alternatively, the local MS can forward the request to the global MS which returns the global GLI-addresses so that GLI-node 1 needs to issue only a single query. Node 1 uses its own local GLI-address as source address and one of the returned global GLI-addresses of ID 3 as destination address for communication with node 3.

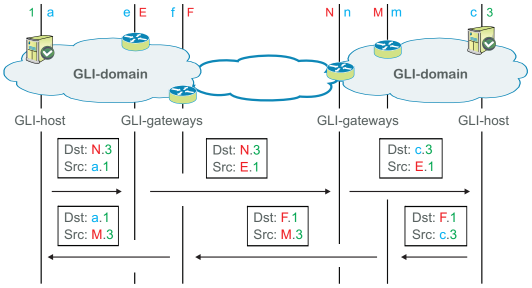

Fig. 3. Communication process with horizontal address translation between two GLI-domains. GLI-node 1 sends a packet to node 3 in a different GLI-domain and node 3 replies.

Figure 3 shows how source and destination address fields of IP packets change on the path between GLI-nodes 1 and 3. Depending on the configuration of the local routing system, packets are forwarded either to a default GLI-gateway or to a specific GLI-gateway. Here we assume that packets are routed to the gateway with GL E. When a GLI-gateway receives a packet destined to an outbound global address, it substitutes the local source address with the global source address reflecting its own GL. Then, the packet contains globally routable source and destination addresses. It can be carried over the

*An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.*

IPv6-Internet backbone via normal BGP interdomain routing towards the GLI-gateway whose GL is reflected in the packet's global destination address. The GLI-gateway in the destination GLI-domain queries its local MS for a local GLI-address of ID 3 and substitutes the global destination GLI-address in the packet by a local destination GLI-address. Based on the local destination GLI-address, the packet is eventually delivered to GLI-node 3.

When GLI-node 3 sends a response back to node 1, it also queries the MS to obtain a GL of ID 1. When GLI-domains are multi-homed, different GLI-gateways may be chosen. As a result, different global GLI-addresses may be used in the two directions of a single communication session (see Figure 3).

B. Transport Layer Implications

We introduce the concept of addressing symmetry, how GLI-Split bypasses this requirement by vertical address translation, and how the use of special GLI-addresses avoids problems with TCP checksum calculation after horizontal or vertical address translation in communication with non-upgraded GLI-nodes.

1) Addressing Symmetry: Transport layer protocols use source and destination IP addresses including port numbers to map packets to flows. Moreover, bidirectional transport protocols or applications expect that packets flowing in the reverse direction (responses) have just interchanged source and destination IP addresses relative to packets flowing in the forward direction (requests) because receivers just swap these addresses when responding. We call this property *addressing symmetry*. In case of multihoming, this property can be easily violated as we observed in Section III-A2. When addresses of returning packets differ from the addresses used by the sender that initiated the connection, these packets cannot be mapped to the existing communication session.

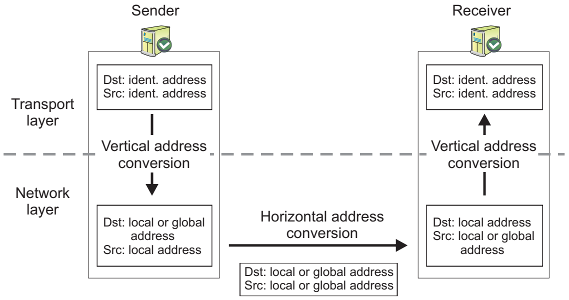

Fig. 4. GLI-nodes translate identifier addresses to local or global addresses when handing data from the transport layer to the network layer and vice-versa.

2) Address Translation between Transport and Network Layer: GLI-Split achieves addressing symmetry by using identifier GLI-addresses on the transport layer and local or global GLI-addresses on the network layer. An upgraded GLI-node translates between both address types when handing data up or down the protocol stack. We call this principle vertical address translation which is illustrated in Figure 4. In contrast, horizontal address translation happens in GLI-gateways on the way from the sender to the receiver.

3) TCP Checksum Compensation: TCP uses a 16-bit checksum in its header and includes the source and destination address of the IP header in the computation. This is a violation of the layering principle, but it must be considered by GLI-Split as TCP is the most used transport protocol. If the source and destination address pair differs on the transport layer at the sender and the receiver, an error likely occurs when the checksum is validated at the receiver. Today's Internet already faces this problem with NAT boxes. To solve the problem, NAT boxes recompute the TCP checksum when they translate addresses. However, this works only under certain conditions. For instance, IPSec makes NAT traversal more difficult since it hides TCP payload from middleboxes so that additional protocols are needed [24].

Horizontal and vertical address translation in GLI-Split change source and destination addresses, too. When two GLI-nodes communicate with each other, checksum problems do not occur because GLI-nodes see only identifier addresses on the transport layer. However, checksum problems possibly occur for communication with non-upgraded nodes because they use locator-dependent GLI-addresses for checksum calculation which are subject to changes. After horizontal and possibly also vertical address translation of GLI-addresses, the higher-order 64 bit locator part of the source and destination address pair is no longer the same so that the corresponding node is likely to calculate a different checksum. GLI-Split solves this problem by compensating these bit changes with an additional checksum inside the GLI-address (see Figure 2). The 16-bits are computed like in the TCP header as the one's complement sum of the preceding 3 16-bit words. Hence, the checksum of the total GLI-address remains the same and changing locators of GLI-addresses in the IP header has no impact on TCP checksums. This makes translation of GLI-addresses invisible to the TCP checksum operation.

C. Gateway Selection and Preservation

When edge networks are multi-homed, traffic may leave or enter through different gateways. First, we propose a mechanism for GLI-nodes to enforce a certain gateway for outgoing packets. Then, we suggest a method for GLI-gateways to preserve the global destination GLI-address of incoming traffic as source GLI-address in outgoing response packets. Both mechanisms require an address buffer to store a single additional GLI-address in the IPv6 header. This address buffer may be implemented by a new IPv6 extension header. It is only used inside a GLI-domain so that the size of external packets is not increased and, thus, cannot cause MTU issues in the Internet.

1) Gateway Selection: We assume a multi-homed GLI-domain with several GLI-gateways. When a GLI-node sends packets to a global address, the local routing system determines the GLI-gateway to which the packets are forwarded. To enforce a certain GLI-gateway for outgoing traffic, the GLI-node stores the global destination address in the address buffer

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

and sends the packet to the selected GLI-gateway, using a global address of the gateway as destination address. If the GLI-gateway receives a packet with an address buffer, it strips off the address buffer and substitutes the destination address of the packet by the address in the address buffer. As usual, the GLI-gateway also replaces the local source address with a global address, reflecting the gateway's GL.

2) Global Address Preservation (GAP): When a destination GLI-domain is multi-homed, packets in the forward direction of a connection may take a different GLI-gateway than packets in the reverse direction. This may result in different global GLI-addresses at the initial sender and to violation of the addressing symmetry principle. When the GAP-bit (see Figure 2) is activated in the global GLI-address of a packet's destination, the GAP-mechanism is triggered at the GLI-gateway of the destination domain to preserve the global destination address of request packets as the global source address of potential response packets. To that end, the GLI-gateway adds an address buffer to the packet storing the currently used global GLI-address of the destination before substituting this address by a local GLI-address. The destination node recognizes the activated GAP-bit of the global GLI-address in the address buffer and stores it. When response packets of the same connection are sent, the GLI-node uses gateway selection for these packets to the respective GLI-gateway. Thereby, addressing symmetry for that connection is enforced at the initial sender.

D. Interworking: GLI-Domains and the Classic IPv6 Internet

Interworking between GLI-domains and the classic IPv6 Internet is challenging because nodes without upgraded networking stacks require addressing symmetry, otherwise they cannot map return data to the appropriate TCP socket. We show that this problem occurs only when the communication is initiated by a non-upgraded node and propose solutions.

1) Communication from a GLI-Domain to the non-GLI IPv6 Internet: When a GLI-node sends a message to a node in the non-GLI IPv6 Internet, it uses its own identifier address as source and the conventional IPv6 address as destination on the transport layer. The source address is as usual replaced by a local address, but the destination address is not changed when passing the packet from the transport to the network layer. The packet is carried to a GLI-gateway which then substitutes the local source address by the global address reflecting the GL of that GLI-gateway. Eventually, the packet is delivered to the destination node. This node can respond to that packet by simply swapping source and destination address. The receiving GLI-node can map the packet as a response to its initial request because addressing symmetry is achieved with the identifier GLI-address and the non-GLI IPv6 address on the transport layer.

2) Communication from the IPv6 Internet to a GLI-Domain: When node 11 (*2001:db8::11*) in the classic IPv6 Internet wants to send a message to GLI-node 3 in a multi-homed GLI-domain (see topology in Figure 5), it uses its IPv6 address as source address and the global GLI-address of node 3, which was obtained through the DNS, as destination address. Since the GLI-domain is multi-homed, response messages may be forwarded through GLI-gateway N or M. Hence, the global GLI-address in the source field of the response messages may differ from the one in the destination field of the packets sent to node 3. Therefore, node 11 may be faced with a violation of addressing symmetry. To avoid that, nodes in the non-GLI IPv6 Internet receive from the DNS only global GLI-addresses with an active GAP-bit when communicating with GLI-nodes. The gateway of the GLI-domain then uses GAP so that response packets use the same GL as previous request packets. The GAP-mechanism is not required in single-homed GLI-domains (e.g. for GLI-node 5 in Figure 1, which can only use GL S anyway)

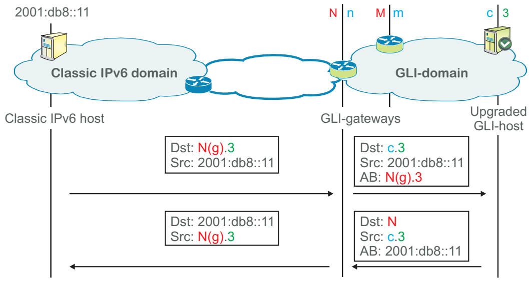

Fig. 5. IPv6 node 2001:db8::11 in a non-GLI domain communicates with GLI-node 3. The destination GLI-domain uses global address preservation and gateway selection based on address buffers (AB) to ensure that outgoing messages use the same GLI-gateway as incoming messages.

E. Multipath Support

When an edge network is multi-homed, its nodes have multiple paths to destinations in other domains, but only a single path can be used in the current Internet. However, networking could benefit from using all available paths [25], [26]. For example, a node could balance traffic over multiple paths to maximize its throughput or it could improve fault tolerance. The Stream Control Transmission Protocol (SCTP) [27] takes advantage of that. Multipath support requires that hosts can determine through which gateway their traffic should be carried. If both the source and the destination network are multi-homed, multipath routing could enforce specific gateways both in the source and destination domain. We explain how this can be achieved with GLI-Split.

A GLI-node queries the global MS for the set of its own global GLI-addresses and the one of its corresponding node. Each combination of global source and destination GLI-addresses represents a different path. These paths are not necessarily entirely disjoint, but possibly on the last mile between the customer and the provider network which is often the slowest and most error-prone part of the path. To send traffic over a specific path, a GLI-node selects the appropriate GLI-gateway for its outgoing traffic (see Section III-C1) and uses the appropriate global GLI-address for the destination node to select a specific GLI-gateway in the destination domain.

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

F. Traffic Engineering Support

A GLI-domain may be connected to two ISPs: to a cheap ISP for carrying its best effort traffic and to an expensive ISP for carrying its premium traffic from demanding applications such as games or live video. In our example in Figure 1, E may be the gateway to the cheap ISP and F may be the gateway to the expensive ISP. Thus, best effort traffic should be exchanged through gateway E while premium traffic should be exchanged through gateway F.

1) Gateway Selection for Self-Initialized Communication: We assume that GLI-node 1 wants to establish a real-time connection with another node outside its own domain. It selects outgoing GLI-gateway F using the method described in Section III-C1. When sending the packet to F, it activates the GAP-bit in the global GLI-address '*F(g).**' to indicate that F should set the GAP-bit in the global source address. Thus, gateway F substitutes the local GLI-address '*a.1*' in the source field of the packet with the global GLI-address '*F(g).1*'. As a result, the corresponding node of node 1 will send return data to '*F(g).1*' and not to another global address of 1. This is important for destination nodes in GLI-domains with upgraded networking stacks as they could send return data to '*E.1*'. Hence, client node 1 has successfully selected gateway F for outgoing and incoming traffic.

2) Gateway Selection for Incoming Traffic: Gateway selection for incoming traffic requires support from the DNS and the global MS. A node may offer different services: one requires best effort transport and another requires premium transport. The DNS name for the best effort service should resolve, e.g., to E(g).1 and the name for the premium service should resolve, e.g., to F(g).10. Nodes without upgraded networking stacks use this information to contact the server. Nodes with upgraded networking stacks use just the destination ID 1 or 10 and query the local or global MS for an appropriate local or global address. Therefore, the global MS should be configured to return E.1 and F.10 as default and F.1 and E.10 as alternative to be used when the default values do not work. This ensures that GLI-nodes with upgraded networking stacks usually contact the best effort service through ID 1 and gateway E and the premium service through ID 10 and gateway F as desired.

G. Mobility Support

In today's Internet, mobile IP is needed for communication with a mobile node (MN). The MN's home address serves as a stable reference address on the transport layer and for finding a rendez-vous point with the MN on the network layer. If the MN leaves its home network, the MN's care-of-address indicates its location on the network layer. With upgraded GLI-nodes, locators in local or global addresses may change due to roaming without breaking transport connections because upgraded GLI-nodes use only identifier addresses on the transport layer so that mobile IP is no longer needed. However, GLI-Split allows improved mobility support only if two upgraded GLI-nodes communicate with each other and reside in GLI-domains. Any other communication patterns are supported by mobile IP.

Mobility support with GLI-Split works as follows. The DNS stores a static home address of the MN which is used for mobile IP. This is a GLI-address and contains the identifier in the usual position. Thus, GLI-nodes can extract the identifier and get an appropriate locator for the MN. When a MN roams into a GLI-domain, it receives new local and global locators and updates the global MS and the local MS in the new domain. Furthermore, it informs all GLI-upgraded corresponding nodes (CNs) about its new global locator with mobility update messages so that the CNs can reach the MN again. The CN may query the local MS to obtain the local locator of the MN to avoid triangle routing via the GLI-gateway just in case that the MN and the CN are in the same GLI-domain (see Section IV-D). Then, both nodes communicate via a direct connection without triangle routing. A similar feature is provided by the proposal in [28]. In contrast to GLI-Split, in this proposal an upgraded MN updates the DNS with its new address when roaming into a new network; interworking methods with non-upgraded nodes were not defined. In GLI-Split, the new global GLI-address of the MN is also used as care-of-address for communication with non-upgraded nodes using mobile IP.

We highlight the benefits of the new mobility support offered by GLI-Split compared to mobile IP. CNs can contact MNs always directly without triangle routing over a home agent. This is an advantage since home agents may be far away and increase the latency. With mobile IPv6, such route optimization can be done under some conditions, but the first contact with the MN is always via the home agent. Furthermore, GLI-Split makes local moves of MNs almost invisible to CNs in other domains. If the MN moves only within a GLI-domain, it receives a different LL but keeps the same GL so that CNs in different domain can continue to send to the same global GLI-address as before. Hence, the communication is hardly impaired by the location change.

H. Security Concerns and Countermeasures

We first consider a problem that is common to all Loc/ID split approaches [29], then another problem that is caused by the introduction of mobility update messages [28] , and finally an issue with gateway preservation methods. Solutions exist for all problems.

1) ID Hijacking through Locator Gleaning: Locator gleaning means that nodes store ID-to-GL mappings in their local caches when they see incoming packets with new ID/GL mappings. This possibly saves queries to the MS, but it causes a security problem so that locator gleaning should be avoided.

Figure 6 illustrates how an attacker can hijack the ID of another node when GLI-hosts use locator gleaning. The attacker behind GLI-gateway X pretends to be node 1. It sends a packet with ID 1 in the source address to node 3. Node 3 receives the global GLI-address X.1 and updates its local cache with the mapping entry 1→X ("locator gleaning"). When node 3 contacts node 1 later, it uses the wrong locator

*An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.*

from the local cache and the packets destined to node 1 will be delivered to the spoofing node behind X instead of the correct node behind E.

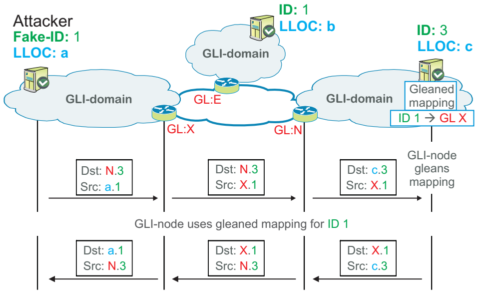

Fig. 6. When a GLI-host gleans locators from incoming source addresses, a malicious node can send a message with a spoofed source ID to that host and steal traffic intended for that ID.

A countermeasure against that type of attack is implemented in the upgraded stack of GLI-nodes and GLI-gateways. When a packet is received with an unknown ID/GL combination in the source address, this mapping should be validated by a query to the MS before storing it in the local cache. Classic IPv6 nodes including those inside a GLI-domain are not affected by wrong mapping information since they are unaware of locators, identifiers, and mappings.

2) Flow Interception through Spoofed Mobility Updates: When two upgraded GLI-nodes in different GLI-domains communicate with each other, a malicious GLI-gateway of another domain can deviate the flows to intercept them. This is illustrated in Figure 7. The attacking GLI-gateway sends a mobility update message to both GLI-nodes, saying that the locator of the other node has changed to the locator of the malicious GLI-gateway. Thus, the attacker attracts the traffic from both nodes and can forward it to the other node. Thereby, the GLI-gateway can intercept the traffic although it is not on the path between the two communicating nodes.

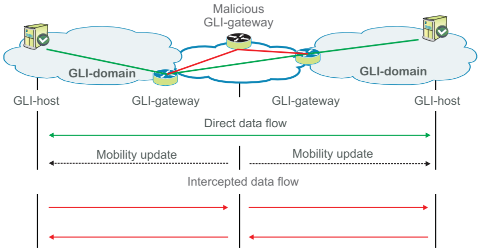

Fig. 7. A malicious GLI-gateway sends spoofed mobility update messages to two communicating GLI-nodes and intercepts their conversation.

This problem can be avoided if mobility update messages are signed by the sender and validated by the receiver. The use of a nonce has been proposed as a solution for that problem in the context of another proposal [28].

3) Flow Interruption through Malicious Updates to GAP: When GAP (Section III-C2) is used for communication from a classic IPv6-host C outside a GLI-domain with a multi-homed GLI-host G, an attacker X might be able to interrupt an ongoing communication session. With GAP, GLI-host G remembers which gateway was used by host C to send packets to G. To send response packets back to C, it uses the same gateway and, thus, the same GL. When attacker X sends a malicious packet with the spoofed source address and port of C to the GLI-host G via a different gateway, G could perform a GAP-update and then use the other gateway for outgoing packets. This violates routing symmetry at host C and packets can no longer be matched to the current communication session.

The described issue can easily be resolved. A GLI-host must not dynamically update the binding between a communication session with a legacy host and the used GLI-gateway. A legacy host usually does not perform a DNS-lookup during an ongoing communication session. Even if such a lookup would be performed, a regular IPv6 host does not know that the "new" address with a different GL belongs to the same GLI-host as before. Instead, it initiates a new communication session with that new address, which uses a different source port. Thus, the GLI-host stores a different binding for this session. Therefore, no dynamic GAP-update is required.

IV. GLI-SPLIT WITH CLASSIC IPV6 NODES

The description of GLI-Split in the previous section requires upgraded networking stacks for GLI-nodes. This is a major obstacle for its initial deployment. Upgrading the nodes can easily be achieved through system updates, which are frequently available for new equipment. However, it is hard to upgrade legacy equipment for which updates are not offered anymore. Thus, for incremental deployability of GLI-Split within GLI-domains it is important to accommodate also classic IPv6 nodes without upgraded networking stacks. We describe additions to GLI-Split for that purpose. We show how the missing functionality of the classic IPv6 stacks can be compensated by modified behavior of the local DNS server and enhanced behavior of the GLI-gateways. We present an alternative mechanism for GAP based on stateful NAT which is used for interworking with the non-GLI Internet. Furthermore, we propose a method to handle local traffic that mistakenly uses global GLI-addresses, which may happen when a global GLI-address was obtained for the destination from a DNS server outside the GLI-domain.

A. Modified Behavior of Local DNS Servers

The DNS is configured to return a global GLI-address with an activated GAP-bit for GLI-nodes. When an upgraded GLI-node wants to contact another node, it receives its global address from the DNS, but uses only the integrated ID to query the local MS for the local or global GLI-addresses. Thereby, an upgraded GLI-node finds out whether the communication peer resides in the GLI-domain so that it uses a local GLI-address of the corresponding node for communication. Classic IPv6 nodes cannot query the MS and rely on the result from the DNS server. Therefore, the local DNS server should

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

return local GLI-addresses for nodes inside its GLI-domain. However, local GLI-addresses should never leave a GLI-domain as they are not routable outside. Therefore, such a modified DNS server must be contacted only from within the GLI-domain.

B. Enhanced Behavior of GLI-Gateways

The local MS knows which hosts inside its domain are upgraded and which are classic IPv6. When a packet arrives at a GLI-gateway, the gateway asks the local MS for a local destination GLI-address of that packet. The local MS returns the requested address and upgrade information to the gateway. Thus, the gateway can behave differently depending on whether it forwards packets to upgraded or classic hosts.

C. NAT-Based Global Address Preservation

When a GLI-gateway receives a packet with an active GAP-bit in the destination address, it must assure addressing symmetry for responses. Upgraded GLI-nodes implement GAP using gateway selection for that objective. Classic IPv6 nodes miss this feature. We show how it can be compensated through stateful network address translation (NAT) by GLI-gateways.

The GLI-gateway keeps a NAT table that maps pairs of external source and destination addresses to pairs of internal source and destination addresses. Furthermore, a part of the ID space is reserved for private use inside GLI-domains that can be used by GLI-gateways to perform NAT. When a GLI-gateway receives an incoming packet for a classic node with the GAP-bit set in the global destination address, it substitutes the source and destination address according to the entries in its NAT table. When no matching entry is found in the NAT table, a new entry is established that maps the external address pair to the corresponding local destination address and a global source address that consists of the LL of the gateway and a currently unused private ID. Response messages from the destination node are returned to the same GLI-gateway which replaces the source and destination addresses according to the entries in its NAT table so that leaving response messages have symmetric source and destination addresses relative to previous request messages.

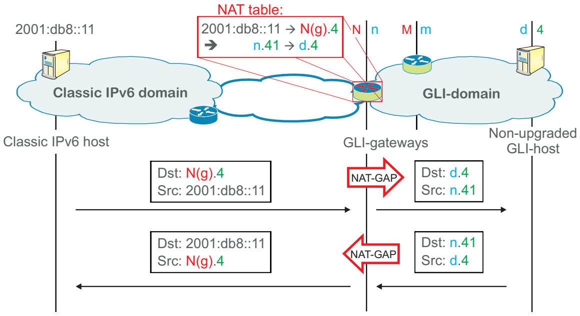

Fig. 8. IPv6 host 2001:db8::11 in a non-GLI-domain communicates with the non-upgraded GLI-node 4 using NAT-based GAP.

Figure 8 illustrates this procedure. GLI-gateway N receives a packet with a global source address 2001:db8::11 and global destination GLI-address '$N(g).4$'. It queries the local MS for a local GLI-address of ID 4 and obtains '$d.4$' as well as the information that node 4 is a classic IPv6 node. Therefore, NAT-based GAP and gateway selection must be applied. The GLI-node searches it NAT-table but does not find a matching entry. Therefore, it picks a currently unused private ID (e.g. 41) and records the mapping (2001:db8::11, '$N(g).4$')→ ('$n.41$','$d.4$') in its NAT table. It translates the source and destination address of the packet accordingly and the packet is delivered to node 4. When response messages from node 4 return to the gateway N, it substitutes the source and destination address in the response packet according to the reverse entry in the NAT table.

D. Handling Local Traffic with Global GLI-Addresses

When a classic IPv6 node in a GLI-domain wants to communicate with another node in the same domain, it should receive a local GLI-address from the DNS. If it accidentally obtains a global GLI-address with a set GAP-bit for such a node from an external DNS, the GLI-gateways have to follow special rules to handle this correctly. We illustrate this using Figure 9. Nodes 3 and 4 are in the same GLI-domain. Node 4 wants to send a packet to node 3 and has obtained a global address of node 3. Unlike an upgraded host, the classic host 4 cannot contact the local MS to find out the correct local address. It just sends a packet with the global GLI-destination-address '*N(g).3*' and the packet is forwarded to the gateway N.

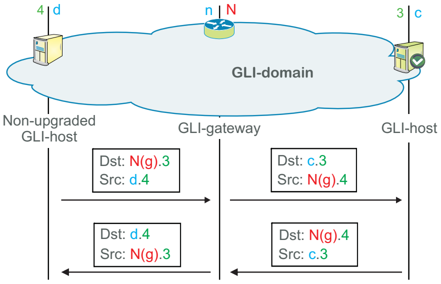

Fig. 9. Reflection of local traffic: classic IPv6-GLI-node 4 communicates with GLI-node 3 via global addresses. The gateway of their GLI-domain reflects the traffic between the hosts to ensure addressing symmetry.

Gateway N recognizes that both sender and receiver of the packet are inside its own GLI-domain. It substitutes the global GLI-address of the destination with an appropriate local GLI-address. The local source address is replaced by a global source address '*N(g).4*', reflecting N as gateway, node 4 as source, and setting the GAP-bit. The packet reaches node 3 and when node 3 responds to that packet, the previously set GAP-bit ensures that addressing symmetry is respected. Thus, also the response message is returned to gateway N. Gateway N handles this packet like the one before so that node 4 receives response messages with the global address of node 3 in the source field. This way, addressing symmetry is achieved and bidirectional communication possible.

The described operation of the gateway is stateless. There is no need to build or store any mapping table. The gateway

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

uses only the information in each packet to translate source and destination addresses.

V. Benefits of GLI-Split

GLI-Split improves the scalability of Internet core routing by removing the need for fine-grained provider-independent addresses and provides many benefits for edge networks. We first summarize the full set of advantages for communication between upgraded GLI-hosts. Then, we analyze which subset thereof is also available for classic IPv6 nodes in GLI-domains.

A. Benefits for Upgraded GLI-Nodes

With GLI-Split, hosts are not configured with any GLs. This simplifies provider changes as it makes renumbering in terms of assigning new GLs obsolete. Renumbering nodes inside a GLI-domain means assigning new LLs. This is useful when subnetworks need to be rearranged for administrative reasons. This is also facilitated since LLs are automatically assigned to nodes. Nodes outside a GLI-domain are unaware of the corresponding local addresses and nodes inside a GLI-domain should use only identifier addresses for configuration purposes which do not change in case of new LLs.

GLI-Split enables multi-homing and takes advantage of all benefits associated with multi-homing. When the connection from the local GLI-domain to its ISP fails, the local routing system reroutes the traffic to another GLI-gateway. When a destination is not reachable at its default locator, the source may be notified about a failure and may address the traffic to another global GLI-address. This represents a host-based rerouting technique which is an alternative to network-based rerouting techniques as presented in [30]. GLI-hosts can select the GLI-gateways of the source and destination domain and thereby enable multipath routing which might be useful for host-based load balancing. Traffic engineering for outbound traffic can be performed by enforcing the GLI-gateway of the source domain with gateway selection. In addition, traffic engineering for inbound traffic can be achieved by enforcing the GLI-gateway of destination domains. This is done by activating the GAP-bit in global GLI-addresses for certain services or nodes. Moreover, GLI-Split provides improved mobility support in the sense that corresponding nodes can contact mobile nodes directly without triangle routing over a home agent.

Most of these advanced networking features are not available in today's Internet or require provider-independent addresses. GLI-Split enables even smallest edge networks to use these features without increasing the routing tables in the DFZ. In contrast to many other future Internet routing proposals, GLI-Split does not suffer from potential problems due to increased packet sizes after encapsulation and it does not require special interworking techniques with the classic IPv6 Internet.

B. Incentives for Early Adopters

GLI-nodes of early adopters usually communicate with the classic Internet which reduces the set of advantages provided by GLI-Split. However, it still has appealing benefits. Multi-homing is still possible. GLI-domains can change providers without renumbering, but global GLI-addresses communicated to external nodes need to be changed. Traffic engineering for outbound and inbound traffic can still be performed.

C. Benefits for Classic IPv6 Nodes in GLI-Domains

Classic IPv6 nodes can be accommodated in GLI-domains. This is a valuable feature for incremental deployability since equipment for which upgraded GLI-networking stacks are not yet available or legacy equipment for which GLI-networking stacks will not be provided anymore can be operated in GLI-domains. Internal renumbering after a provider change is facilitated because classic IPv6 nodes in GLI-domains know only their local GLI-address. Hence, provider changes are invisible to them like to nodes behind a NAT-gateway. Multi-homing is possible. When communicating with upgraded GLI-nodes, they can perform host-based rerouting so that also classic IPv6 nodes in multi-homed GLI-domains get better resiliency. Traffic engineering is supported for incoming traffic but not for outbound traffic.

VI. Related Work

There are various other proposals for new routing and addressing architectures trying to solve the scalability problem of today's Internet. We review only those implementing a Loc/ID split in some form but not those tweaking today's BGP, e.g. [31]. The authors of [32] identified two different strategies: *separation* of core and edge networks and *elimination* of de-aggregated provider-independent and provider-aggregatable addresses from BGP routing tables. First we review separation approaches, then an elimination approach, and an example where the Loc/ID split is used without the intention to solve the Internet's scalability problem. Finally, we compare general NAT and GLI-Split.

Proposals implementing separation can be subdivided into address rewriting, map-and-encaps, and source routing approaches. With address rewriting, border routers add global locator information to packets destined for a different domain by coding this information into source and destination addresses for transit purposes. GLI-Split falls into that class. Also Six/One Router [9], [33] uses address rewriting. Identifiers are only locally routable addresses. When communicating with nodes in different domains, the addresses are rewritten 1-to-1 through stateless NAT in border routers to globally routable transit addresses. A major focus of Six/One Router is improved multi-homing support. The Identifier Locator Network Protocol (ILNP) [10], [34], [35] is similar to GLI-Split in the sense that it splits the IPv6 address into a locator and identifier part, but there are many differences. With ILNP, applications are expected to identify nodes only by fully qualified domain names (FQDNs) and the DNS resolves them to possibly several addresses containing the unique identifier of a node and a locator. The lookup is done by the hosts and no gateway interaction is required. Hosts must be upgraded to take advantage of ILNP since gateways cannot take over

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.

partial functions as in GLI-Split. GLI-Split, ILNP, and Six/One Router have evolved from the early ideas of GSE (global, site, and end-system address elements) [36], [37]. It essentially codes a global locator, a local locator, and an identifier into an IPv6 address. Addresses are dynamically combined from these parts. It uses only the identifier for TCP checksum calculation and requires host upgrades for deployment. IP Next Layer (IPNL) [13] uses fully qualified domain names as identifiers, and introduces a so-called IPNL layer between the transport and the networking layer, thus requiring host upgrades. It is based on NAT and works with IPv4.

The Hierarchical Architecture for Internet Routing (HAIR) [16] is a clean-slate approach and does not need address rewriting by border routers. It implements source routing in the sense that the hosts compose destination addresses containing global locator, local locator, and identifier information. That requires host upgrades since hosts need to perform mapping lookups for that purpose.

With map-and-encaps, border routers add global locator information to packets destined to a different domain by tunneling them across the Internet backbone to the gateway with a specific global locator [38]. This requires an additional IP header which increases the IP packet size and can cause MTU issues. There are several proposals that are intended to be incrementally deployed in the Internet: e.g. LISP [7], [39], TRRP [40], APT [11], [12], IVIP [8]. The locator/identifier separation protocol (LISP) is the most prominent of them. The IP address of a LISP-gateway is a global locator and routable in the Internet backbone. Addresses of LISP-nodes inside LISP-domains are locally routable endpoint identifiers. Interworking with the classic Internet may be done using stateful NAT or proxy gateways. Stateful NAT is complex and we explain the problems with proxy gateways. LISP-nodes can send packets directly to classic nodes in the general Internet outside LISP-domains. When a classic node sends packets to a node within a LISP-domain, the packets are forwarded by default to a proxy router in the Internet which looks up appropriate global locators and tunnels the packets to the destination LISP-domain using this locator information. Proxy routers have two major disadvantages. First, traffic cannot take the shortest AS-path but takes a detour via the proxy (triangle routing). Second, they attract and forward large data volumes and it is not clear who pays for it. Similar interworking solutions exist also for other map-and-encaps proposals. GLI-Split is intentionally designed to avoid these problems.

There are also clean-slate map-and-encaps schemes which require fundamental changes to the Internet. The Node Identity Internetworking Architecture (NIIA) [14], [41] uses non-routable node IDs as identifiers. The Hierarchical Routing Architecture (HRA) [15] is very similar. Map-and-encaps schemes have difficulties to support multipath routing or host-based traffic engineering because hosts cannot influence the gateway's choice of global locators.

An example for an elimination scheme is Shim6 [42]. Multi-homed hosts have several IP addresses, one from each ISP, and can use them independently or as backups during failures. They do not have a stable identifier, thus provider changes are more complex, and mobility is not supported. According to [32], elimination schemes in general have several disadvantages compared to separation approaches.

The Host Identity Protocol (HIP) [43] also implements the Loc/ID split. However, its intention is rather enhanced anonymity, security, and mobility instead of improved routing scalability. It could be used on top of other approaches to combine their advantages.

NAT66 [44] describes network address translation between IPv6 addresses. GLI-gateways could take advantage of this specification. In this light, GLI-Split seems like doing large-scale NAT for edge networks, but there are significant differences between conventional NATs and GLI-Split. Hence, conventional stateful NAT and GLI-Split must not be confounded. Thanks to the mapping system, the NAT operation performed by GLI-gateways is stateless and nodes in GLI-domains are reachable by global addresses. GLI-Split even improves their reachability beyond provider changes.

VII. CONCLUSION

GLI-Split implements the Loc/ID split concept within today's IPv6 Internet. Thereby, it can solve the scalability problem for a future IPv6 Internet when prefixes of global GLI-addresses are adopted for core routing. In addition, it provides many benefits to users in GLI-domains. They can change providers without internal renumbering, multi-homing is facilitated even for smallest GLI-domains and can be exploited for multipath forwarding, traffic engineering, improved reliability and mobility support. GLI-Split is incrementally deployable on a per-domain basis and also within a single domain the migration from non-upgraded GLI-nodes to upgraded GLI-nodes can be done gradually. GLI-gateways perform simple address rewriting without the need for session state. This also holds for interworking with the classic IPv6 Internet. In contrast to many other proposals, GLI-Split does not need triangle routing via extra devices for that purpose. Although the full set of benefits is available only for communications among GLI-nodes with upgraded networking stacks, GLI-Split provides advantages for upgraded GLI-nodes when communicating with the classic IPv6 Internet and even for classic IPv6 nodes in GLI-domains. These are important deployment incentives for early adopters and prerequisite for incremental deployment.

ACKNOWLEDGEMENTS

The authors would like to thank Christian Vogt for fruitful and stimulating discussions and Phuoc Tran-Gia, Rolf Winter, Bryan Ford, Bengt Ahlgren, Javier Ubillos, Robin Whittle, and Michael Hoefling for their excellent feedback to improve the paper.

REFERENCES

[1] X. Meng, Z. Xu, B. Zhang, G. Huston, S. Lu, and L. Zhang, "IPv4 Address Allocation and the BGP Routing Table Evolution," *ACM SIGCOMM Computer Communications Review*, vol. 35, no. 1, pp. 71 – 80, Jan. 2005.

[2] D. Meyer, L. Zhang, and K. Fall, "RFC4984: Report from the IAB Workshop on Routing and Addressing," Sep. 2007.

[3] G. Huston, "IPv4 Address Report, generated daily," http://www.potaroo.net/tools/ipv4/, 2010.

[4] B. Quoitin, L. Iannone, C. de Launois, and O. Bonaventure, "Evaluating the Benefits of the Locator/Identifier Separation," in *ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Kyoto, Japan, Aug. 2007.

[5] O. Bonaventure, "Reconsidering the Internet Routing Architecture," in *Routing Research Group Seminar at IETF-68*, Prague, Czech Republic, Mar. 2007.

[6] T. Li (ed.), "Design Goals for Scalable Internet Routing," http://tools.ietf.org/id/draft-irtf-rrg-design-goals, Jul. 2007.

[7] D. Meyer, "The Locator Identifier Separation Protocol (LISP)," *The Internet Protocol Journal*, vol. 11, no. 1, pp. 23–36, Mar. 2008.

[8] R. Whittle, "IVIP - A New Routing and Addressing Architecture for the Internet," www.firstpr.com.au/ip/ivip/, 2008.

[9] C. Vogt, "Six/One Router: A Scalable and Backwards Compatible Solution for Provider-Independent Addressing," in *ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Seattle, WA, USA, Aug. 2008.

[10] R. Atkinson, S. Bhatti, and S. Hailes, "Harmonised Resilience, Security and Mobility Capability for IP," in *IEEE Military Communications Conference (MILCOM)*, 2008.

[11] D. Jen, M. Meisel, D. Massey, L. Wang, B. Zhang, and L. Zhang, "APT: A Practical Tunneling Architecture for Routing Scalability," UCLA Computer Science Department, Tech. Rep. 080004, Mar. 2008. [Online]. Available: http://fmdb.cs.ucla.edu/Treports/080004.pdf

[12] D. Massey, L. Wang, B. Zhang, and L. Zhang, "A Scalable Routing System Design for Future Internet," in *ACM International Workshop on IPv6 and the Future of the Internet (IPv6)*, Kyoto, Japan, Aug. 2007.

[13] P. Francis and R. Gummadi, "IPNL: A NAT-Extended Internet Architecture," in *ACM SIGCOMM*, San Diego, CA, Aug. 2001.

[14] B. Ahlgren, J. Arkko, L. Eggert, and J. Rajahalme, "A Node Identity Internetworking Architecture," in *IEEE Global Internet Symposium*, Barcelona, Spain, Apr. 2006.

[15] X. Xu and D. Guo, "Hierarchical Routing Architecture (HRA) ," in *Conference on Next Generation Internet Design and Engineering (NGI)*, Krakow, Poland, Apr. 2008.

[16] A. Feldmann, L. Cittadini, W. Mühlbauer, R. Bush, and O. Maennel, "HAIR: Hierarchical Architecture for Internet Routing," in *Re-Architecting the Internet (ReArch)*, Rome, Italy, Dec. 2009.

[17] O. Hanka, C. Spleiss, G. Kunzmann, and J. Eberspächer, "A Novel DHT-Based Network Architecture for the Next Generation Internet," in *International Conference on Networking (ICN)*, Cancun, Mexico, Mar. 2009.

[18] S. Jiang, "Hierarchical Host Identity Tag Architecture," http://tools.ietf.org/html/draft-jiang-hiprg-hhit-arch-03, Oct. 2009.

[19] L. Iannone and O. Bonaventure, "Locator/ID Separation: Study on the Cost of Mappings Caching and Mappings Lookups," Université Catholique de Louvain, Tech. Rep. 2007-04, 2007.

[20] L. Mathy and L. Iannone, "LISP-DHT: Towards a DHT to Map Identifiers onto Locators," in *Re-Architecting the Internet (ReArch)*, Madrid, Spain, Dec. 2008.

[21] H. Luo, Y. Qin, and H. Zhang, "A DHT-Based Identifier-to-Locator Mapping Scheme for a Scalable Internet," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 10, Oct. 2009.

[22] V. Fuller, D. Farinacci, D. Meyer, and D. Lewis, "LISP Alternative Topology (LISP+ALT)," http://tools.ietf.org/html/draft-ietf-lisp-alt-03, Mar. 2010.

[23] V. Fuller and D. Farinacci, "LISP Map Server," http://tools.ietf.org/html/draft-ietf-lisp-ms-04, Oct. 2009.

[24] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, and M. Stenberg, "RFC3948: UDP Encapsulation of IPsec ESP Packets," Jan. 2005.

[25] D. Wischik, M. Handley, and M. Bagnulo Braun, "The Resource Pooling Principle," *ACM SIGCOMM Computer Communications Review*, Oct. 2008.

[26] J. He and J. Rexford, "Towards Internet-wide Multipath Routing," *IEEE Network Magazine*, Mar. 2008.

[27] R. Steward (ed.), "RFC4960: Stream Control Transmission Protocol," Sep. 2007.

[28] R. Atkinson, S. Bhatti, and S. Hailes, "ILNP: Mobility, Multi-Homing, Localised Addressing and Security through Naming," *Telecommunication Systems*, vol. 42, no. 3-4, pp. 273–291, Oct. 2009.

[29] D. Saucez, L. Iannone, and O. Bonaventure, "Notes on LISP Security Threats and Requirements," http://tools.ietf.org/html/draft-saucez-lisp-security, Oct. 2009.

[30] P. Francois, C. Filsfils, and O. Bonaventure, "Achieving Sub-50 Milliseconds Recovery Upon BGP Peering Link Failures," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1123–1135, Dec. 2007.

[31] X. Zhang, P. Francis, J. Wang, and K. Yoshida, "Scaling IP Routing with the Core Router-Integrated Overlay," in *IEEE International Conference on Network Protocols (ICNP)*, 2006.

[32] D. Jen, M. Meisel, H. Yan, D. Massey, L. Wang, B. Zhang, and L. Zhang, "Towards a New Internet Routing Architecture: Arguments for Separating Edges from Transit Core," in 7^{th} *ACM Workshop on Hot Topics in Networks (HotNets)*, Calgary, Alberta, Canada, Oct. 2008.

[33] C. Vogt, "Six/One Router - Design and Motivation," http://users.piuha.net/chvogt/pub/2008/vogt-2008-six-one-router-design.pdf, Jul. 2008.

[34] R. Atkinson, S. Bhatti, and S. Hailes, "A Proposal for Unifying Mobility with Multi-Homing, NAT, & Security," in *ACM International Workshop on Mobility and Wireless Access (MobiWac)*, Chania, Crete Island, Greece, 2007.

[35] ——, "Mobility as an Integrated Service through the Use of Naming," in *ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Chania, Crete Island, Greece, 2007.

[36] M. O'Dell, "GSE - An Alternate Addressing Architecture for IPv6," http://tools.ietf.org/id/draft-ietf-ipngwg-gseaddr-00.txt, Feb. 1997.

[37] L. Zhang, "An Overview of Multihoming and Open Issues in GSE," *IETF Journal*, vol. 2, no. 2, Autumn 2006.

[38] R. Hinden, "RFC1955: New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG," Jun. 1996.

[39] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/ID Separation Protocol (LISP)," http://tools.ietf.org/html/draft-ietf-lisp-06, Jan. 2010.

[40] W. Herrin, "Tunneling Route Reduction Protocol (TRRP)," http://bill.herrin.us/network/trrp.html, 2008.

[41] S. Schuetz, H. Abrahamsson, B. Ahlgren, and M. Brunner, "Design and Implementation of the Node Identity Internetworking Architecture," Swedish Institute of Computer Science, Kista, Sweden, SICS Technical Report, No. T2008:1, 2008.

[42] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," http://tools.ietf.org/id/draft-ietf-shim6-proto, Feb. 2009.

[43] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "RFC5201: Host Identity Protocol," Apr. 2008.

[44] M. Wassermann and F. Baker, "IPv6-to-IPv6 Network Address Translation (NAT66)," http://tools.ietf.org/html/draft-mrw-behave-nat66, Nov. 2008.

An updated version of this technical report has been published in the MDPI Future Internet open access journal.
The document is available via https://www.mdpi.com/1999-5903/5/1/67.