Future Internet **2013**, *5*, 67-94; doi:10.3390/fi5010067

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

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

Michael Menth [1,*], Matthias Hartmann [2] and Dominik Klein [2]

[1] Department of Computer Science, University of Tuebingen, Sand 13, 72076 Tuebingen, Germany

[2] Chair of Communication Networks, Institute of Computer Science, University of Wuerzburg, Am Hubland, 97074 Wuerzburg, Germany; E-Mails: hartmann@informatik.uni-wuerzburg.de (M.H.); dominik.klein@informatik.uni-wuerzburg.de (D.K.)

* Author to whom correspondence should be addressed; E-Mail: menth@uni-tuebingen.de; Tel.: +49-7071-29-70505; Fax: +49-7071-29-5220.

Received: 15 January 2013 / Accepted: 4 March 2013 / Published: 11 March 2013

Abstract: The locator/identifier split is an approach for a new addressing and routing architecture to make routing in the core of the Internet more scalable. Based on this principle, we developed the GLI-Split framework, which separates the functionality of current IP addresses into a stable identifier and two independent locators, one for routing in the Internet core and one for edge networks. This makes routing in the Internet more stable and provides more flexibility for edge networks. GLI-Split can be incrementally deployed and it is backward-compatible with the IPv6 Internet. We describe its architecture, compare it to other approaches, present its benefits, and finally present a proof-of-concept implementation of GLI-Split.

Keywords: locator/identifier split; scalable core routing; multihoming

1. Introduction

Typical BGP (border gateway protocol) routing tables in the default-free zone (DFZ) of the Internet currently hold about 400,000 entries and continue to grow ever 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 is already exhausted [3]. We believe that this will lead to increased IPv6 deployment. IPv6 has room for a multitude of addresses and might cause an immense 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 hardware and software upgrades. Therefore, the modified Internet architecture should also satisfy additional requirements like support for renumbering, multihoming, multipath transmission, or security [5,6].

Most of the current proposals for a future routing and addressing architecture [7] 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, e.g., [8], but they take a clean-slate approach, *i.e.*, they are not backward-compatible with today's Internet which makes them difficult 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 of 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. GLI-Split, however, does more than only solve the scalability problem. It also has several compelling benefits: it facilitates provider changes, renumbering, multihoming, multipath-routing, traffic engineering, and provides improved mobility support. To take full advantage of all features, nodes in GLI-domains require upgraded networking stacks, but legacy nodes can also be accommodated in GLI-domains and enjoy benefits. This facilitates incremental deployability. For interworking between GLI-Split and the IPv4 Internet, we can use existing mechanisms for IPv4 and IPv6, as GLI-Split is IPv6-compatible.

This paper is structured as follows. Section 2 presents general building blocks for new addressing schemes, gives a high-level introduction to GLI-Split, and discusses related works. Section 3 presents fundamentals of GLI-Split and explains how GLI-Split works with upgraded and non-upgraded nodes in single-homed domains. Section 4 then introduces mechanisms required for the multihomed case and describes how multipath transfer and traffic engineering can be supported. Section 5 briefly introduces our implementation of the GLI-Split architecture and presents a proof-of-concept evaluation with respect to the round-trip-time. Finally, we summarize the benefits of GLI-Split and discuss deployment considerations in Section 6 and conclude the work in Section 7.

2. A New Routing Architecture

One of the general principles for a more scalable Internet is the *separation* of core and edge networks [9] in terms of routing and address space. By removing the edge network prefixes from the routing tables in the DFZ, dynamic changes in the routing space of edge networks are hidden and

remain local. The routing tables in the DFZ then grow with the small number of core networks and not with the number of edge networks. This separation principle requires a new addressing and routing architecture which can be realized in many different ways. We explain the basic design options for such an architecture and use them to classify GLI-Split. Then, we give an overview of related architectures and compare them to our approach.

2.1. Architectural Design Options

A distinctive feature of a separation architecture is the location *where* the separation of core and edge addressing takes place. In a host-based architecture, each participating host performs the separation. Packets on the transport layer are addressed with identifiers and the protocol that handles the separation adds locators before the packets leave the host. On the network, only locators are used to forward packets. In a network-based architecture, on the other hand, identifiers are used both on transport and network layer inside a host, while the translation from identifiers to locators is done inside the network at a middlebox, e.g., a border router. In mixed architectures, both options are used and there is a separation at the host and at a network middlebox. The location of the separation and, thus, the entity that requires mappings from identifier to locator has direct influence on the design of the mapping system, which we studied in [10].

Another design question is *how* the separation is implemented. One option is map-and-encaps [11], where global locator information is added to packets destined to a different domain by tunneling them across the Internet backbone to the gateway with a specific global locator. This requires an additional IP header which increases the IP packet size and can cause MTU issues. An alternative is address rewriting, where global locator information is added to packets destined for a different domain by coding this information into source and destination addresses. The last option is source routing, whereby locator and identifiers are encoded by the source host in the destination address. In this case, no modifications of packets along the path to the destination are necessary.

In addition, it is important to decide which *advanced mechanisms* or services should be natively supported by the architecture that are not directly required for the plain architecture to work. This could be, for example, support for interworking, mobility, multipath routing, or traffic engineering, as well as built-in security. All these options have direct influence on the design of the architecture and may influence each other so that a multitude of different scenarios has to be considered. Hence, care has to be taken when choosing the right combination of design options.

The *GLI-Split architecture* is a separation scheme which uses address rewriting to translate between identifiers and routing locators. The separation is done both at hosts and at border routers. Hosts use identifier addresses on the transport layer and *local* routing locator addresses on the network layer. Border routers then translate between *local* and *global* routing locator addresses. Due to this mixed architecture, mapping lookups are done both at hosts and at border routers. GLI-Split natively supports communication with classic IPv6 nodes and implements features to support mobility, multihoming, traffic engineering, and multipath transfer.

2.2. Previous Approaches

There is a multitude of architectures for the future Internet and, in particular, for a new routing and addressing architecture, trying to solve the scalability problem of today's Internet [12]. In the following, we review prominent architectures in this research area, show which design options have been chosen, and address some of their shortcomings.

The Identifier Locator Network Protocol (ILNP) [13–15] 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 Domain Name System (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 partial functions as in GLI-Split. GLI-Split and ILNP have evolved from the early ideas of GSE (global, site, and end-system address elements) [16,17]. GSE 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.

The Hierarchical Architecture for Internet Routing (HAIR) [8] 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.

There are several proposals that are intended to be incrementally deployed in the Internet. The locator/identifier separation protocol (LISP) [18,19] 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 complex stateful NAT or 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.

The Host Identity Protocol (HIP) [20] 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.

NPTv6 [21] describes network address translation between IPv6 addresses. GLI-gateways could take advantage of this specification. In this light, GLI-Split resembles large-scale NAT for edge networks, but there are significant differences. 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.

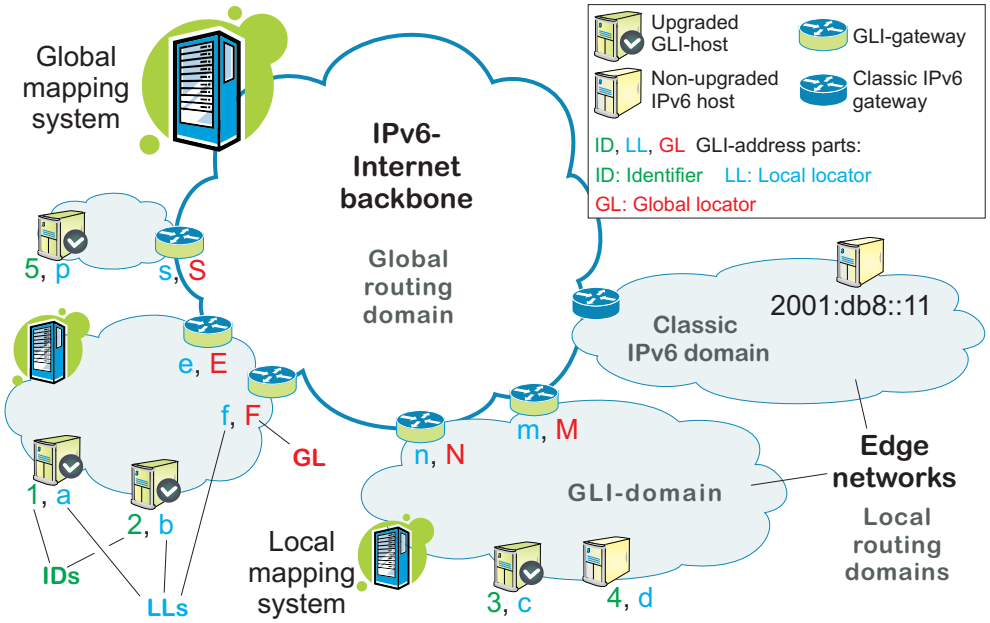
3. Fundamentals of GLI-Split

This section introduces the basic nomenclature, shows the GLI address structure, and explains their relation to DNS.

3.1. General Idea and Nomenclature

Edge networks like those of companies that implement GLI-Split are called GLI-domains while others are called *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 system (MS) maps IDs to global locators and a local mapping system maps IDs to local locators. This setting is illustrated in Figure 1. IDs are denoted by integral numbers, local locators by lowercase letters, and global locators 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.

Figure 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.



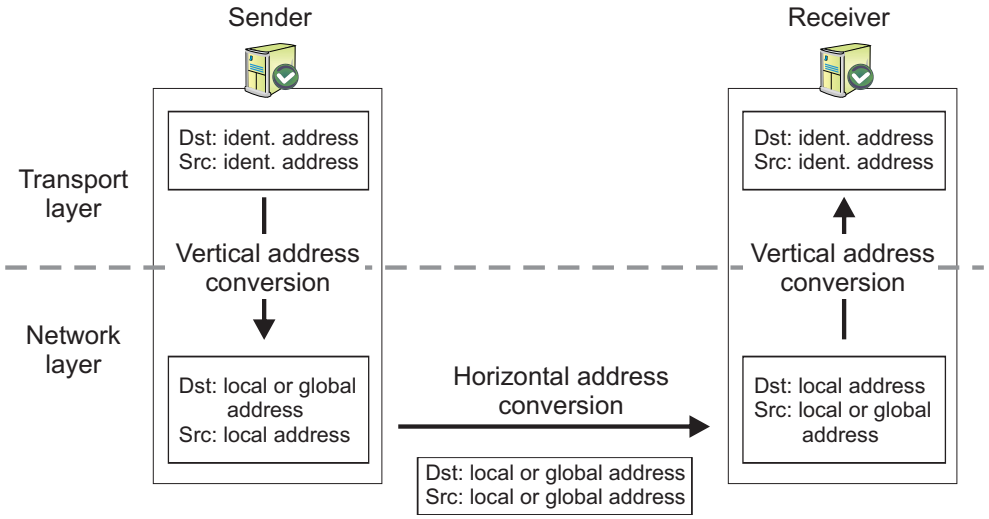
3.2. GLI-Addressing

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 included locator, we distinguish three types of addresses: identifier addresses, local addresses, and global addresses.

Transport layer protocols like TCP use source and destination IP addresses to map packets to flows. During an ongoing transport connection, these elements must not change; otherwise, packets cannot be mapped correctly to the existing connection. An *identifier address* is an endpoint identifier, independent of any locator information, which is used in the transport layer of upgraded GLI-nodes. This guarantees that regardless of the current location of the upgraded GLI-node, the transport layer sees the same address. On the network layer, locator addresses are used to encode the current location. An upgraded GLI-node translates between both address types when handing data up or down the protocol stack. This principle is called vertical address translation and illustrated in Figure 2. Depending on the scope of the locator address, we distinguish between two different types. A *local address* is used for forwarding within a GLI-domain. As the local locator has only site-local meaning, a local address must never leave a GLI-domain. To ensure this requirement, a responsible GLI-gateway at the border of the host's GLI-domain translates between local addresses and global addresses. This property is called horizontal address translation and can also be seen in Figure 2.

Figure 2. GLI-nodes translate identifier addresses to local or global addresses when handing data from the transport layer to the network layer and *vice versa*.



A *global address* is mainly used for routing outside GLI-domains. The global locator 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.

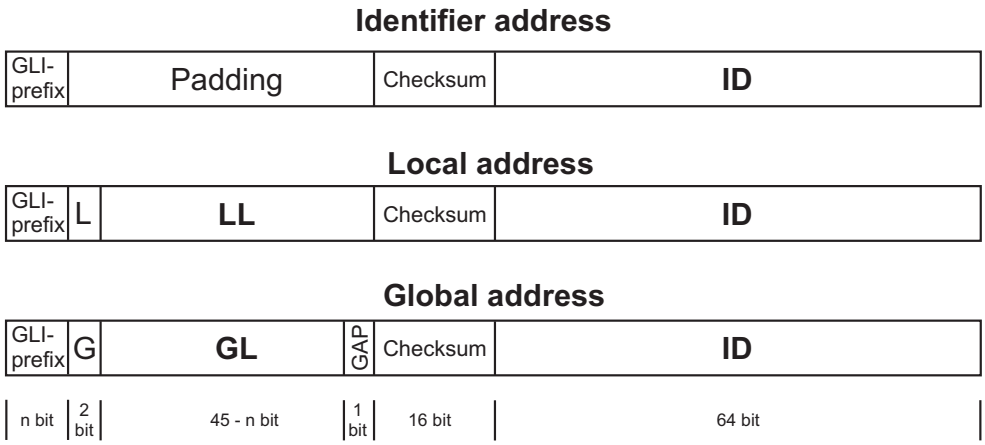
Inside a GLI-domain, packets addressed to global addresses are usually forwarded to a default gateway. However, if the global locator in the destination address belongs to a GLI-gateway of the same GLI-domain, the packet is routed to that GLI-gateway.

3.2.1. Address Format

Figure 3 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. A similar separation is done by ILNP [22]. All GLI-addresses have a special n-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. 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 (see Section 4.2.2). Identifier addresses have the locator field filled with padding zeros.

Figure 3. Three types of GLI-addresses are encoded in an IPv6 address.



3.2.2. Address Assignment

The remaining 16 bits are used for checksum compensation so that checksums calculated, e.g., by TCP, are still valid after locator changes. TCP uses a 16-bit checksum in its header and includes the source and destination address of the IP header in the computation.

Horizontal and vertical address translation in GLI-Split change source and destination addresses. 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. GLI-Split solves this problem by compensating these bit changes with an additional checksum inside the GLI-address (see Figure 3). The 16-bits are computed like in the TCP header as the one's complement sum of the preceding three 16-bit words. Therefore, changing a GLI-address does not modify the TCP checksum. This makes translation of GLI-addresses invisible to TCP checksum operations.

Global locators 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 of any routing information. The hierarchy here is important to improve the scalability of the mapping system, which can then work with ID-prefixes instead of individual IDs.

HIP-like IDs may be also supported using the concept in [23]. Local locators 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 local locators to nodes inside a GLI-domain may be done by enhanced DHCP. This DHCP also communicates the information on how to reach the mapping service. An upgraded GLI-node knows its ID, informs the DHCP, which then returns a local locator, as well as a set of global locators. The upgraded GLI-node registers the ID-to-LL and ID-to-GL mappings with the local and global mapping system, 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 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 that reflects 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 mapping system. As a consequence, stateless address auto configuration [24] cannot be used in this case.

3.2.3. Notation

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

3.3. Name Resolution

To start a communication session, the initiating host resolves a DNS name (e.g., host3.other-gli-domain.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 system to find an appropriate local or global locator for the ID.

3.3.1. Use of the DNS

When a DNS name denotes a GLI-node in a multihomed domain, it returns a global GLI-address with a set GAP-bit (see Section 4.2.2). If the DNS name belongs to a GLI-node in a single-homed domain, the GAP-bit is not set. In both cases, the returned GLI-address is globally routable and hosts outside of GLI-domains can use this address without modifications. This requires no changes to the currently used DNS servers in the Internet. More details about multihomed domains are provided in Section 4.

3.3.2. Use of the Mapping System

The mapping system consists of a local and a global component. The local mapping system stores a set of local GLI-addresses for IDs residing within its local GLI-domain while the global mapping system 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 mapping system when the ID belongs to a GLI-node in a multihomed 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 mapping system for an appropriate GLI-address. If the destination node resides in the same GLI-domain as the requesting node, the local mapping system 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 mapping system which returns a set of global GLI-addresses.

Like the DNS, the mapping system 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 mapping system becomes a performance bottleneck [25]. We do not specify how the mapping system works in detail but in [10], we propose a scalable, reliable, and secure mapping system called FIRMS which could be used in combination with GLI-Split. In addition in [26], we propose a classification of current mapping systems and compare FIRMS with many others, e.g., [27–30], in detail.

3.4. Communication between Upgraded GLI-Nodes

In this section, we describe the communication between two GLI-nodes with upgraded networking stacks and how networking details are hidden from the transport layer. In the examples, GLI-node 1 establishes communication with another GLI-node with the DNS name hostX.exampleY.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.

3.4.1. Communication within a GLI-Domain

GLI-node 1 communicates with GLI-node 2 in the same GLI-domain (see Figure 1). Node 1 queries the local mapping system for a local GLI-address of ID 2. As both GLI-nodes are part of the same GLI-domain, the mapping system 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.

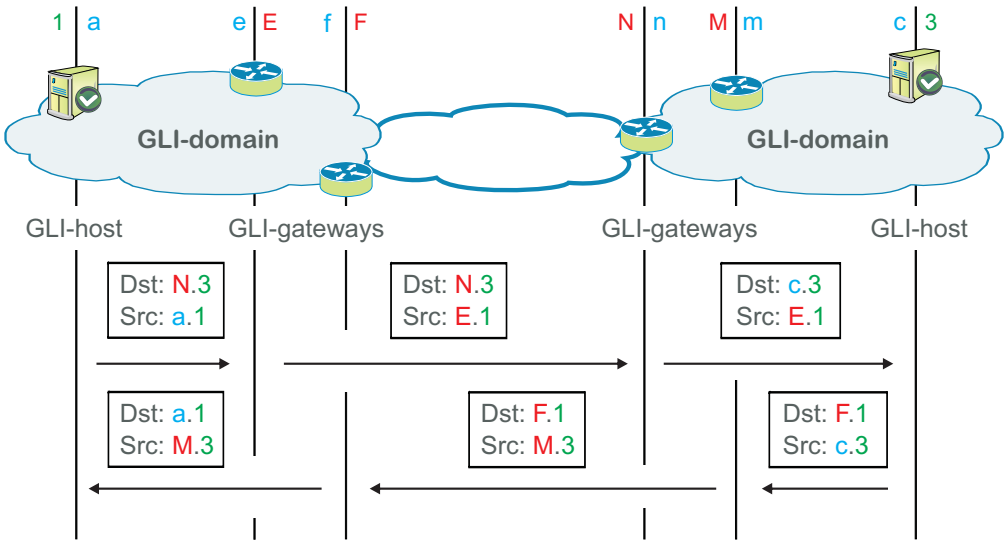
3.4.2. Communication between GLI-Domains

GLI-node 1 communicates with GLI-node 3 in a different GLI-domain (see Figure 1). When node 1 queries the local mapping system for local GLI-addresses of ID 3, it receives a negative answer. Then, node 1 queries the global mapping system for a global GLI-address of ID 3. Alternatively, the local mapping system can forward the request to the global mapping system, 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.

Figure 4 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. We assume that packets are routed to the gateway with global locator 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 global locator. Then, the packet contains globally routable source and destination addresses. It can be carried over the standard IPv6-Internet backbone towards the GLI-gateway whose global locator is reflected in the packet's global destination address. The GLI-gateway in the destination GLI-domain queries its local mapping system 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.

Figure 4. 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.



When GLI-node 3 sends a response back to node 1, it also queries the mapping system to obtain a global locator of ID 1. When GLI-domains are multihomed, 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 4). This example demonstrates that GLI-Split is by design able to utilize different paths for domains with several gateways. However, if access control or filtering devices like firewalls require that packets enter and leave the GLI-domain through the same GLI-gateway, this can be supported by the mechanisms described in Sections 4.2.1. and 4.2.2.

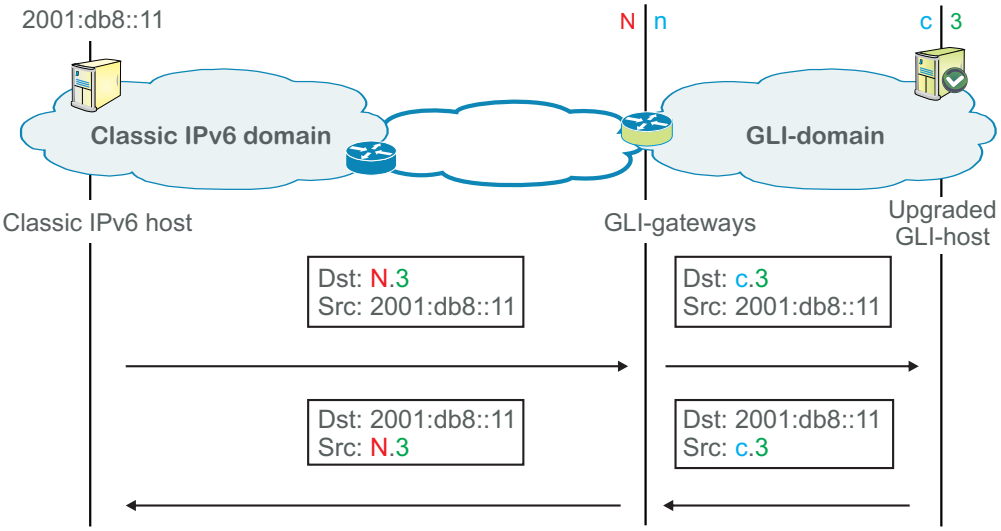
3.5. Interworking between GLI-Domains and the Classic IPv6 Internet

For future Internet routing architectures, it is extremely important that the communication with the non-upgraded part of the Internet is possible and that it does not imply any restrictions. In the GLI-Split architecture, the interworking between single-homed GLI-domains and classic IPv6 domains is natively supported. In multihomed networks, some additional mechanisms are required, which are explained in Section 4.

In the single-homed case, when node 11 (*2001:db8::11*) in the classic IPv6 Internet wants to initiate a communication to the GLI-node 3 in a 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. According to the global locator N in the global GLI-address, the packet is delivered to the GLI-gateway of the destination GLI-domain. There, the GLI-gateway queries the local mapping system for the local locator of the destination GLI-node and replaces the global GLI-address in the destination field with the returned local GLI-address. The packet is then forwarded according to the local locator to the destination node. At GLI-node 3, the local GLI-address on the network layer is replaced by an identifier address before handing the packet up to the transport layer. This is the vertical address translation mechanism which is explained in Section 3.2. In return packets, GLI-node 3 simply swaps source and destination address on network layer and sends the packet to its default GLI-gateway. There, the local GLI-address in the source field is replaced with a global GLI-address indicating the global locator of the GLI-gateway. After the translation, the packet is forwarded according to the classic IPv6 address in the destination field and eventually arrives at node 11 in the classic IPv6 domain.

Figure 5. IPv6 node with IP address 2001:db8::11 in a non-GLI domain communicates with GLI-node 3 in GLI-domain.



In the opposite direction, when a GLI-node initiates a communication 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 global locator 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 the identifier GLI-address and the non-GLI IPv6 address are used on the transport layer.

3.6. Mobility Support

In today's Internet, mobile IP is needed for communication with a mobile node (MN). The mobile node's home address serves as a stable reference address on the transport layer and for finding a rendezvous point with the mobile node on the network layer. If the mobile node leaves its home network, the mobile node'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 mobile node 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 mobile node. When a mobile node roams into a GLI-domain, it receives new local and global locators and updates the global mapping system and the local mapping system 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 corresponding nodes can reach the mobile node again. If the mobile node and the corresponding nodes are in the same GLI-domain, the corresponding nodes may query the local mapping system to obtain the local locator of the mobile node to avoid triangle routing via the GLI-gateway (see Section 4.3.4). Then, both nodes communicate via a direct connection without triangle routing. A similar feature is provided by ILNP [22]. In contrast to GLI-Split, an upgraded mobile node in ILNP updates the DNS with its new address when roaming into a new network; interworking with non-upgraded nodes is not defined. In GLI-Split, the new global GLI-address of the mobile node 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. Corresponding nodes can contact mobile nodes 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 mobile node is always via the home agent. Furthermore, GLI-Split makes local moves of mobile nodes almost invisible to corresponding nodes in other domains. If the mobile node moves only within a GLI-domain, it receives a different local locator but keeps the same global locator so that corresponding nodes in different domains can continue to send to the same global GLI-address as before. Hence, the communication is hardly impaired by the location change.

3.7. Multicast Support

At present, video streaming, IPTV, and content delivery networks account for a large and still growing fraction of Internet traffic. In this area, IP multicast is gaining more and more popularity. We therefore explain how IP multicast traffic is handled with GLI-Split. IPv6 offers native support for multicast and requires the Multicast Listener Discovery (MLD) protocol [31] and the Protocol Independent Multicast-Sparse Mode (PIM-SM) protocol [32]. MLD is used by hosts to join or leave a multicast

group while PIM-SM is used between routers to build the multicast delivery tree state. PIM-SM creates unidirectional trees which are rooted at a group specific rendezvous point. The multicast delivery model can be either any-source multicast (ASM) or source-specific multicast (SSM). The ASM mode relates to many-to-many group communications while the SSM mode relates to one-to-many group communications. In the ASM mode, a host uses the (*,G) state to join all sources in the multicast group with multicast IPv6 address G. In contrast in the SSM mode, a host uses the (S,G) state to join only the source with IPv6 address S in the multicast group with IPv6 multicast address G.

In PIM-SM, multicast group join requests are sent towards the rendezvous point for which the address may be obtained from the multicast group address [33]. In GLI-split, the address of the rendezvous point is a global address so that also classic IPv6 nodes in non GLI-domains are able to join the multicast group. By sending the PIM-SM join request towards the rendezvous point, the required (S,G) state is established in all routers on the path from the receiver to the rendezvous point. In case the rendezvous point is in a GLI-domain, the GLI-gateway translates the address of incoming PIM-SM join requests to the local address of the rendezvous point. To send multicast data to the multicast group, the source forwards the data to the rendezvous point which further distributes the multicast data according to the established (S,G) tree state. In this way, no modifications are required for PIM-SM and MLD, and multicast handling is the same as in the ordinary IPv6 architecture.

3.8. Security Concerns and Countermeasures

In this section, we consider new security threats that arise due to the separation of identity and location information, and show how GLI-Split manages these problems.

3.8.1. Potential New Attacks

The Loc/ID-split-related issues can be generally classified as redirection attacks which constitute threats against confidentially, integrity, and availability [34]. The general idea of these attacks is that an attacker manipulates the information in the mapping components like the mapping cache in order to redirect existing flows to a new target. There, the packets of the redirected flow may either be just dropped to cancel the availability of a service, they could be monitored to violate confidentially, or the contents of the packets could be changed to break the integrity of the transferred data. These issues apply to all protocols where a mapping from an identifier to several locators is used. Examples are threats related to IPv6 multihoming [34], multipath TCP [35], or other new routing architectures like LISP [36].

The threats can be divided into control-plane and data-plane threats. Control-plane threats involve map request and map reply messages. Map request messages could be used for amplifying DoS attacks where an attacker requests mapping information under a spoofed locator address. This locator address is the address of the victim which might then receive a possibly large amount of mapping information. A small map request message from the attacker thus causes a possible large map reply message to the victim. Another threat which involves map request messages is the cache update mechanism that is, for example, used by the mobility extension LISP-MN [37]. This mechanism could be used to either insert false mapping information or to cause a cache overflow. These threats related to the mapping cache

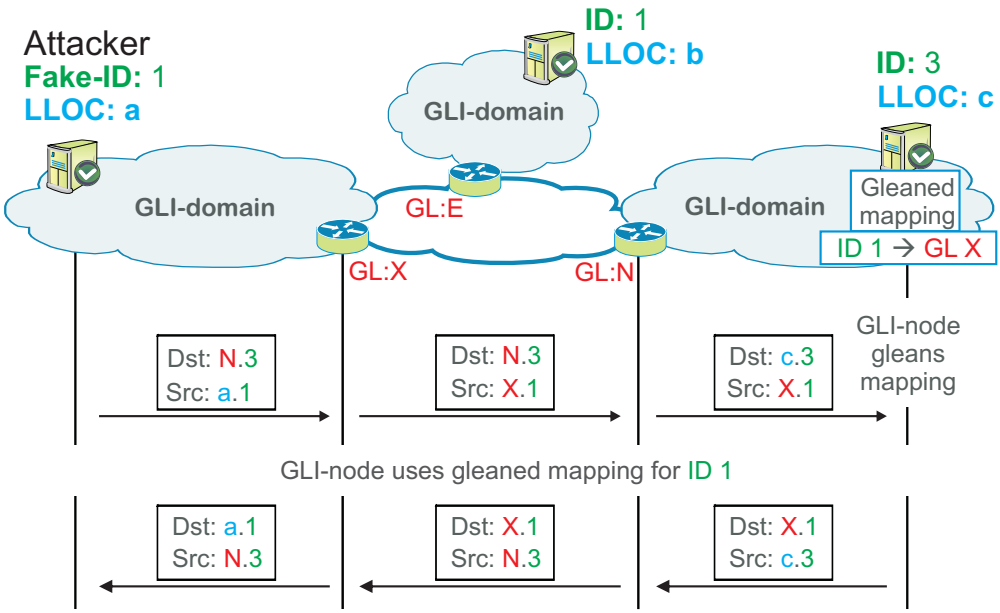
could also be achieved by utilizing the locator gleaning concept on the data-plane. Locator gleaning was proposed by LISP and should reduce the amount of necessary mapping lookups and hence speed up the initial communication establishment.

In the following, we provide more details about the threats related to locator gleaning and mobility update mechanisms and explain, how they can be avoided.

3.8.2. 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 mapping service, 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 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.

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



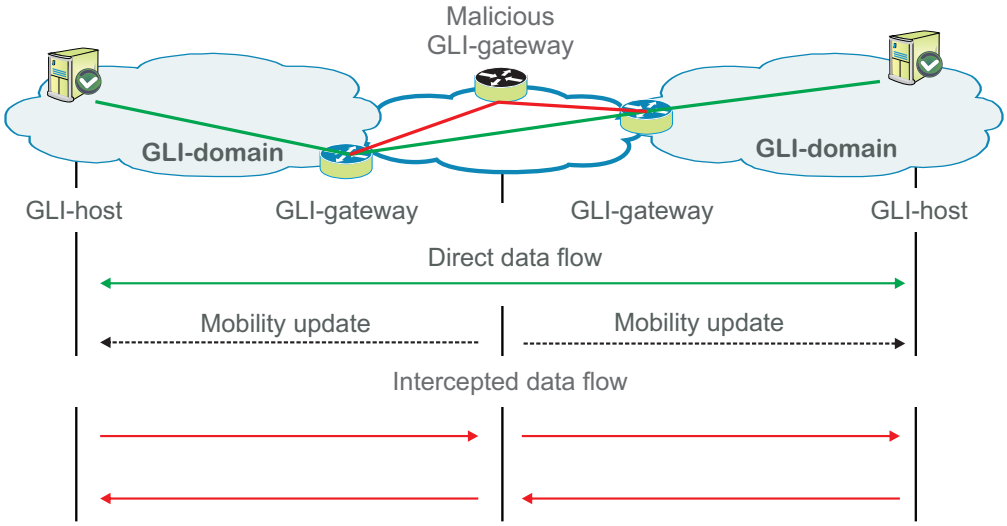
A countermeasure against that type of attack is implemented in the upgraded stack of GLI-nodes and GLI-gateways. When a packet is received with an unknown ID/GL combination in the source address, this mapping should be validated by a query to the mapping service before storing it in the local cache. 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.

3.8.3. 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. The GLI-gateway can thereby intercept the traffic, even though it is not on the path between the two communicating nodes.

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 ILNP [22].

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



4. Multihoming and Interworking

In Section 3, we have introduced the fundamental building blocks of the GLI-Split architecture considering only single-homed GLI-domains. In the multihomed case, some additional mechanisms are required, especially for supporting communications with classic IPv6 nodes either in classic IPv6 domains or in GLI-domains. In the following section, we first briefly explain the issues in the multihomed case and then introduce mechanisms to solve these problems. After that, we introduce advanced mechanisms which facilitate several paths like multipath transfer and traffic engineering.

4.1. Issues with Classic IPv6 Nodes

As explained in Section 3.2, 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. In case of multihoming, this property can be

easily violated as we observed in Section 3.4.2. 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. This is not a problem for upgraded GLI-nodes, as only identifier addresses are used on the transport layer, and changes on the network layer do not affect existing transport connections. However a classic IPv6 node sees these changes on the transport layer and, hence, mechanisms are required to ensure that the addresses do not change when different paths are used.

4.2. Gateway Selection and Preservation

When edge networks are multihomed, 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.

4.2.1. Gateway Selection

We assume a multihomed GLI-domain with several GLI-gateways. When a GLI-node sends packets to a global address, the local routing system inside the local GLI-domain determines the outgoing 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 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 global locator.

4.2.2. Global Address Preservation (GAP)

When a destination GLI-domain is multihomed, 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 the violation on the transport layer explained in Section 4.1. When the GAP-bit (see Figure 3) 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, the initial sender just sees swapped source and destination addresses and no violations on the transport layer occur.

4.3. GLI-Split with Classic IPv6 Nodes

The description of GLI-Split in Section 3 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 also accommodate 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 in the mulithomed case. 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.

4.3.1. Modified Behavior of Local DNS Servers

The DNS is configured to return a global GLI-address with an activated GAP-bit for GLI-nodes in a multihomed domain. 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 mapping system for the local or global GLI-addresses. Subsequently, an upgraded GLI-node finds out whether the communication peer resides in the GLI-domain in order to use a local GLI-address of the corresponding node for communication. Classic IPv6 nodes cannot query the mapping system and rely on the result from the DNS server. Therefore, the local DNS server should 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 from the outside. Such a modified DNS server must therefore be contacted only from within the GLI-domain. This may, for instance, be achieved by checking whether the source address is a local address.

4.3.2. Enhanced Behavior of GLI-Gateways

Upgraded GLI-nodes directly register at the local mapping system and for classic IPv6 nodes, the registration is done, e.g., by an enhanced DHCP (see Section 3.2.2). Hence, the local mapping system 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 mapping system for a local destination GLI-address of that packet. The local mapping system returns the requested address and upgrade information to the gateway. The gateway can thus behave differently, depending on whether it forwards packets to upgraded or classic hosts.

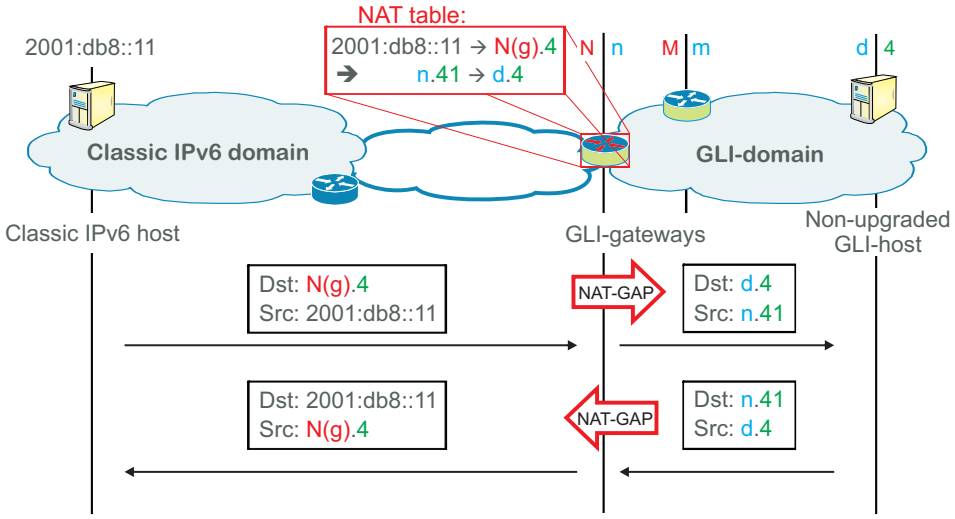
4.3.3. NAT-Based Global Address Preservation

When a GLI-gateway receives packets with an active GAP-bit in the destination address, it must assure that source and destination address are simply swapped and do not change for responses. To achieve this,

upgraded GLI-nodes implement GAP using gateway selection. Classic IPv6 nodes lack 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 local locator 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.

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 mapping system 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 its 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.

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

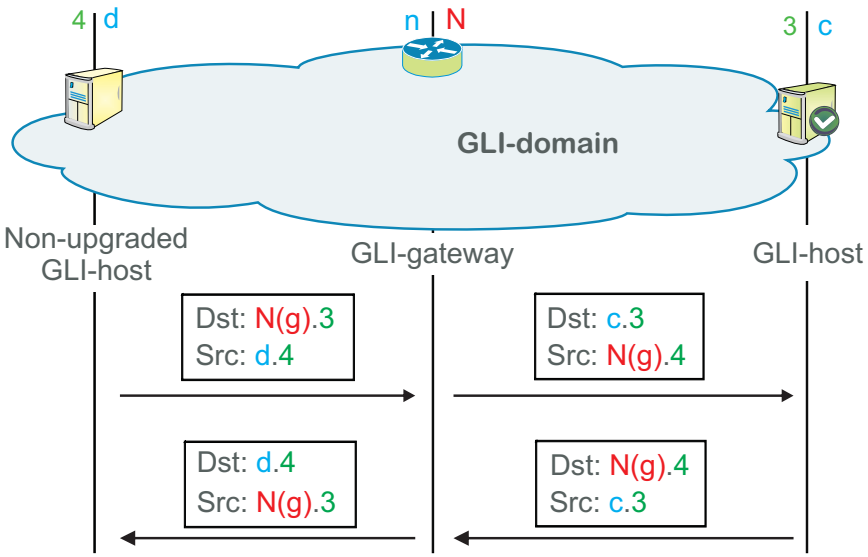


4.3.4. Local Traffic with Global GLI-Addresses

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 mapping system 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.

Figure 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 source and destination address are simply swapped. 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, bidirectional communication is possible. The described operation of the gateway is stateless. There is no need to build or store any mapping table. The gateway uses only the information in each packet to translate source and destination addresses.

4.4. Multipath Support

When an edge network is multihomed, 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 [38,39]. For example, a node could balance traffic over multiple paths to maximize its throughput or it could improve fault tolerance [40,41]. The Stream Control Transmission Protocol (SCTP) [42] 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 multihomed, multipath routing could enforce specific gateways both in the source and destination domain. With GLI-Split this can be achieved as follows. A GLI-node queries the global mapping system 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 disjointed, but possibly so 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 4.2.1.) and uses the appropriate global GLI-address for the destination node to select a specific GLI-gateway in the destination domain.

4.5. Traffic Engineering Support

A GLI-domain might be mulithomed to two ISPs: a cheap ISP for carrying its best-effort traffic, and 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.

4.5.1. 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 4.2.1. 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.

4.5.2. Gateway Selection for Incoming Traffic

Gateway selection for incoming traffic requires support from the DNS and the global mapping system. 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 mapping system for an appropriate local or global address. Therefore, the global mapping system should be configured to return E.1 and F.10 as the default and F.1 and E.10 as the 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.

5. GLI-Split Implementation

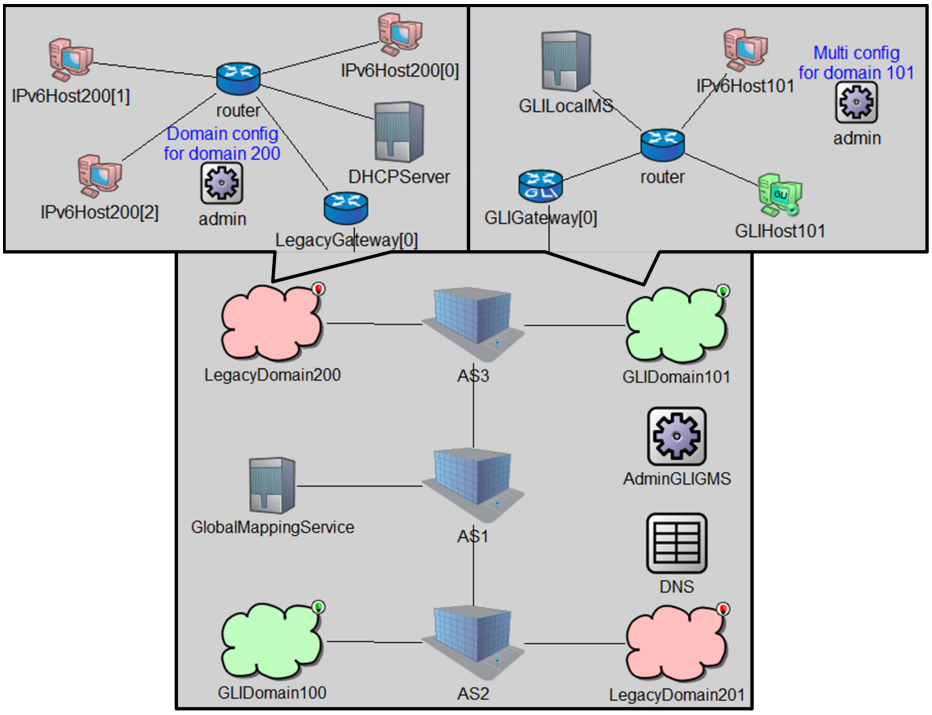
The previous sections described all building blocks, concepts, and algorithms that together form the GLI-Split architecture. As a first demonstration that this concept actually works, we implemented GLI-Split as a proof-of-concept simulation [43] in the INET Framework [44] for OMNeT++ [45]. In this section, we describe the simulation and then use it to present a brief evaluation of the round-trip-time in different communication scenarios.

5.1. OMNeT++ Simulation

OMNeT++ is a modular simulation environment which can be applied to all problem domains where the discrete event- based approach is suitable. Especially for communication networks, the INET Framework for OMNeT++ offers all required communication protocols to model TCP/IPv6 based networks.

Figure 10 shows an example network in INET with single-homed GLI-domains, as well as classic IPv6 domains.

Figure 10. GLI-Split architecture in the INET Framework for OMNeT++ with GLI-domains and classic IPv6 domains.



The different domains are connected via three provider networks. A global DNS module ensures DNS-name-to-global-locator address resolution. Each domain has an administration module (admin) which configures the identifier and local locator prefixes per domain and installs required routing entries. On the global area, a similar administration module configures the global locators per domain and installs inter-domain routing entries. The GLI modules in the implemented model of our GLI-Split architecture comprise the GLI-gateways, as well as local and global mapping servers. Each GLI-domain has its own

local mapping server and there is one global mapping server for the entire network which serves as interface to the mapping service. In the following, this test network is used to present a brief evaluation with respect to the round-trip-time for communications between different domains.

5.2. Round-Trip-Time Evaluation

For the evaluation, all inter-domain link delays in the test network (see Figure 10) have been set to *2 ms*. In the following, we take a brief look at the round-trip-time (RTT) in all six possible combinations of source and destination nodes (see Table 1). In the first four scenarios, no mapping lookups are required and, hence, the RTT just comprises the corresponding inter-domain link delays. This base delay applies to all six combinations and comprises the eight single link delays back and forth between source and destination domain. In the fifth scenario, a classic IPv6 host in a GLI-domain communicates with a GLI-host in another GLI-domain. In this case in the return direction, the GLI-host performs a mapping lookup because the returned address from the DNS is a GLI-address. This results in an additional delay of *12 ms* for the initial message. For a subsequent message, the mapping has already been cached and no further lookups are required. The largest RTT occurs in the last scenario, where two GLI-hosts in different domains communicate. This time, a lookup at each domain is required which adds two times *12 ms* to the base delay. However, this again applies only to the first messages. While this result may seem contradictory, the evaluation does not consider the advanced mechanisms which can be utilized by upgraded GLI-nodes. The next section explains some of these in detail.

Table 1. Comparison of initial and second RTT between classic hosts (H_C) and GLI-hosts (H_{GLI}) in GLI-domains (D_{GLI}) or classic domains (D_C).

Connection	1st RTT	2nd RTT
H_C in $D_C \rightarrow H_C$ in D_C	16 ms	16 ms
H_C in $D_C \rightarrow H_C$ in D_{GLI}	16 ms	16 ms
H_C in $D_C \rightarrow H_{GLI}$ in D_{GLI}	16 ms	16 ms
H_C in $D_{GLI} \rightarrow H_C$ in D_{GLI}	16 ms	16 ms
H_C in $D_{GLI} \rightarrow H_{GLI}$ in D_{GLI}	28 ms	16 ms
H_{GLI} in $D_{GLI} \rightarrow H_{GLI}$ in D_{GLI}	40 ms	16 ms

6. Benefits and Deployment Considerations of GLI-Split

GLI-Split improves the scalability of Internet core routing by removing the need for fine-grained provider-independent addresses and, moreover, provides many benefits for edge networks. We first summarize the full set of advantages for communication between upgraded GLI-hosts before analyzing which subset thereof is also available for classic IPv6 nodes in GLI-domains. Finally, we present required changes to the existing IPv6 architecture and discuss deployment considerations.

6.1. Benefits for Upgraded GLI-Nodes

With GLI-Split, hosts are not configured with any global locators. This simplifies provider changes as it makes renumbering in terms of assigning new global locators obsolete. Renumbering nodes inside a GLI-domain means assigning new local locators. This is necessary, for example, when subnetworks need to be rearranged for administrative reasons. With GLI-Split, this is facilitated because local locators are automatically assigned to nodes and nodes outside a GLI-domain are unaware of the corresponding local addresses. Nodes inside a GLI-domain use only stable identifier addresses for configuration and connection establishment.

GLI-Split enables multihoming and takes advantage of all benefits associated with multihoming. 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 that is an alternative to network-based rerouting techniques, as presented in [46]. 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.

6.2. 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. Multihoming 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.

6.3. 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 no longer be provided, can be operated in GLI-domains.

Internal renumbering after a provider change is simplified because classic IPv6 nodes in GLI-domains know only their local GLI-address. Hence, provider changes are invisible to them, as are nodes behind a NAT-gateway.

Multihoming is possible. When communicating with upgraded GLI-nodes, they can perform host-based rerouting so that also classic IPv6 nodes in multihomed GLI-domains achieve better resiliency. Traffic engineering is supported for incoming traffic but not for outbound traffic.

6.4. Implementation and Deployment Considerations

The GLI-Split functionality inside upgraded GLI-nodes requires host updates that could be distributed via operating system updates. The modification introduces an additional shim layer between the network layer and the transport layer, which performs the vertical address translation (see Section 3.2), as well as mapping registration and mapping lookups for outgoing packets (see Section 3.3.2). The modifications inside hosts do not require changes to transport layer protocols like TCP, as the horizontal address translation done by the shim layer is transparent to upper layers.

In the initial deployment phase, host updates are not necessarily required for all nodes in a GLI-domain, as GLI-Split also accommodates classic IPv6 nodes (see Section 4.3). To achieve this accommodation, a modified DNS is required which returns either a local or a global address, depending on whether source and destination host are in the same or different GLI-domains (see Section 4.3.1). The modification, however, does not require changes to the DNS protocol, as it could be realized via configuring a split-horizon or split-view DNS that provides different DNS records, depending on the location of the querying source host. The only protocol modification that is required is the extension of the DHCPv6 protocol, which is used for the assignment of local addresses to hosts inside GLI-domains (see Section 3.2.2). The DHCP needs to return the address of the local and global mapping service which could be realized via a new DHCP options field, as is currently done for DNS server addresses. A new DHCP options field may also be used to return a set of global locators to upgraded GLI-nodes. For classic IPv6 nodes, the DHCP needs to know the ID and MAC address to compute local GLI-addresses with checksum compensation. In addition, the DHCP is responsible to register the advertised local GLI-addresses in the local mapping service and the corresponding global GLI-addresses in the global mapping service (see Section 3.2.2), which requires an extension of the DHCP server functionality.

The most critical entity in GLI-Split is the GLI-gateway which implements the main network functionality. It is responsible for the horizontal address translation (see Section 3.2) as well as for all mapping service related mechanisms like mapping registration or mapping lookups. Furthermore, it realizes all mechanisms which are required to support classic IPv6 nodes in GLI-domains (see Section 4.3). The complexity of such a GLI-gateway is comparable to a common NAT-gateway, which also translates addresses and recomputes TCP checksums. NAT functionality is, in the current Internet, mostly used in residential home gateways or in carrier-grade or large scale NAT solutions in provider networks. Large scale NAT solutions are, for instance, used in the IPv6 transition mechanisms like NAT444 [47]. Hence, we assume that the complexity of the GLI-Split mechanisms can be handled by available off-the-shelf routing hardware. In addition, we assume that GLI-gateways are located closer to

the edge which also reduces the size of GLI-domains and thus the amount of traffic that must be handled by GLI-gateways.

7. Conclusions

GLI-Split implements the Loc/ID split concept within today's IPv6 Internet, thereby solving the scalability problem for a future IPv6 Internet when prefixes of global GLI-addresses are adopted for core routing. Moreover, it provides many benefits to users in GLI-domains. They can change providers without internal renumbering, and multihoming is facilitated even for the smallest GLI-domains and can be exploited for multipath forwarding, in addition to 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. We demonstrated the incremental deployability of GLI-Split by means of a proof-of-concept implementation in OMNeT++. 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 prerequisites for incremental deployment.

Acknowledgments

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.

This work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (support code 01 BK 0800, G-Lab).

References

1. Zhao, X.; Pacella, D.; Schiller, J. Routing scalability: An operator's view. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 1262–1270.
2. Meyer, D.; Zhang, L.; Fall, K. RFC4984: Report from the IAB Workshop on Routing and Addressing. Available online: http://tools.ietf.org/html/rfc4984 (accessed on 4 March 2013).
3. Huston, G. IPv4 Address Report. Available online: http://www.potaroo.net/tools/ipv4/ (accessed on 4 March 2013).
4. Quoitin, B.; Iannone, L.; de Launois, C.; Bonaventure, O. Evaluating the Benefits of the Locator/Identifier Separation. In Proceedings of the ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch), Kyoto, Japan, 27 August 2007.
5. Bonaventure, O. Reconsidering the Internet Routing Architecture. Presented at The Internet Engineering Task Force IETF-68, Prague, Czech Republic, 18–23 March 2007.

6. Li, T. RFC6227: Design Goals for Scalable Internet Routing. Available online: http://tools.ietf.org/html/rfc6227 (accessed on 4 March 2013).
7. Li, T. RFC6115: Recommendation for a Routing Architecture. Available online: http://tools.ietf.org/html/rfc6115 (accessed on 4 March 2013).
8. Feldmann, A.; Cittadini, L.; Mühlbauer, W.; Bush, R.; Maennel, O. HAIR: Hierarchical Architecture for Internet Routing. In Proceedings of Re-Architecting the Internet (ReArch), Rome, Italy, 1 December 2009.
9. Jen, D.; Meisel, M.; Yan, H.; Massey, D.; Wang, L.; Zhang, B.; Zhang, L. Towards a New Internet Routing Architecture: Arguments for Separating Edges from Transit Core. In Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets), Calgary, Alberta, Canada, 6–7 October 2008.
10. Menth, M.; Hartmann, M.; Hoefling, M. FIRMS: A mapping system for future internet routing. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 1326–1331.
11. Hinden, R. RFC1955: New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG. Available online: http://tools.ietf.org/html/rfc1955 (accessed on 4 March 2013).
12. Paul, S.; Pan, J.; Jain, R. Architectures for the future networks and the next generation Internet: A survey. *Comput. Commun.* **2011**, *34*, 2–42.
13. Atkinson, R.; Bhatti, S.; Hailes, S. A Proposal for Unifying Mobility with Multi-Homing, NAT, & Security. In Proceedings of the ACM International Workshop on Mobility and Wireless Access (MobiWac), Crete Island, Greece, 22 October 2007.
14. Atkinson, R.; Bhatti, S.; Hailes, S. Mobility as an Integrated Service through the Use of Naming. In Proceedings of the ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch), Kyoto, Japan, 27 August 2007.
15. Atkinson, R.; Bhatti, S.; Hailes, S. Evolving the internet architecture through naming. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 1319–1325.
16. O'Dell, M. GSE-An Alternate Addressing Architecture for IPv6. Available online: http://tools.ietf.org/html/draft-ietf-ipngwg-gseaddr (accessed on 4 March 2013).
17. Zhang, L. An overview of multihoming and open issues in GSE. *IETF J.* **2006**, *2*, 29–35
18. Meyer, D. The locator identifier separation protocol (LISP). *Int. Protocol J.* **2008**, *11*, 23–36.
19. Farinacci, D.; Fuller, V.; Meyer, D.; Lewis, D. Locator/ID Separation Protocol (LISP). Available online: http://tools.ietf.org/html/draft-ietf-lisp (accessed on 4 March 2013).
20. Moskowitz, R.; Nikander, P.; Jokela, P.; Henderson, T. RFC5201: Host Identity Protocol. Available online: https://tools.ietf.org/html/rfc5201 (accessed on 4 March 2013).
21. Wassermann, M.; Baker, F. IPv6-to-IPv6 Network Address Translation (NAT66). Available online: http://tools.ietf.org/html/draft-mrw-behave-nat66 (accessed on 4 March 2013).
22. Atkinson, R.; Bhatti, S.; Hailes, S. ILNP: Mobility, multi-homing, localised addressing and security through naming. *Telecommun. Syst.* **2009**, *42*, 273–291.
23. Jiang, S. Hierarchical Host Identity Tag Architecture. Available online: http://tools.ietf.org/html/draft-jiang-hiprg-hhit-arch (accessed on 4 March 2013).
24. Thomson, S.; Narten, T.; Jinmei, T. RFC4862: IPv6 Stateless Address Autoconfiguration. Available online: http://tools.ietf.org/html/rfc4862 (accessed on 4 March 2013).

25. Iannone, L.; Bonaventure, O. On the Cost of Caching Locator/ID Mappings. In Proceedings of the ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT), Kyoto, Japan, 27–31 August 2007.
26. Menth, M.; Hartmann, M.; Hoefling, M. *Mapping Systems for Loc/ID Split Internet Routing*; Technical Report No. 472; University of Würzburg: Würzburg, Germany, 2010.
27. Jakab, L.; Cabellos-Aparicio, A.; Coras, F.; Saucez, D.; Bonaventure, O. LISP-TREE: A DNS hierarchy to support the lisp mapping system. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 1332–1343.
28. Mathy, L.; Iannone, L. LISP-DHT: Towards a DHT to Map Identifiers onto Locators. In Proceedings of Re-Architecting the Internet (ReArch), Madrid, Spain, 9 December 2008.
29. Luo, H.; Qin, Y.; Zhang, H. A DHT-based identifier-to-locator mapping scheme for a scalable Internet. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *20*, 1790–1802.
30. Farinacci, D.; Fuller, V.; Meyer, D.; Lewis, D. LISP Alternative Topology (LISP+ALT), 2011. Available online: http://tools.ietf.org/html/draft-ietf-lisp-alt (accessed on 4 March 2013).
31. Holbrook, H.; Cain, B.; Haberman, B. RFC4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast. Available online: http://tools.ietf.org/html/rfc4604 (accessed on 4 March 2013).
32. Fenner, B.; Handley, M.; Holbrook, H.; Kouvelas, I. RFC4601: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised). Available online: http://tools.ietf.org/html/rfc4601 (accessed on 4 March 2013).
33. Savola, P.; Haberman, B. RFC3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address. Available online: http://tools.ietf.org/html/rfc3956 (accessed on 4 March 2013).
34. Nordmark, E.; Li, T. RFC4218: Threats Relating to IPv6 Multihoming Solutions. Available online: http://tools.ietf.org/html/rfc4218 (accessed on 4 March 2013).
35. Bagnulo, M. RFC6181: Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses. Available online: http://tools.ietf.org/html/rfc6181 (accessed on 4 March 2013).
36. Saucez, D.; Iannone, L.; Bonaventure, O. LISP Threats Analysis. Available online: http://tools.ietf.org/html/draft-ietf-lisp-threats (accessed on 4 March 2013).
37. Farinacci, D.; Lewis, D.; Meyer, D.; White, C. LISP Mobile Node. Available online: http://tools.ietf.org/html/draft-meyer-lisp-mn (accessed on 4 March 2013).
38. Wischik, D.; Handley, M.; Bagnulo Braun, M. The resource pooling principle. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 47–52.
39. He, J.; Rexford, J. Towards internet-wide multipath routing. *IEEE Netw. Mag.* **2008**, *22*, 16–21.
40. Menth, M.; Martin, R.; Hartmann, M.; Spoerlein, U. Efficiency of routing and resilience mechanisms in packet-switched communication networks. *Eur. Trans. Telecommun.* **2010**, *21*, 108–120.
41. Gyarmati, L.; Cinkler, T.; Trinh, T.A. Path-based multipath protection: Resilience using multiple paths. *Trans. Emerg. Telecommun. Technol.* **2012**, *23*, 660–671.
42. Steward, R. RFC4960: Stream Control Transmission Protocol. Available online: http://tools.ietf.org/html/rfc4960 (accessed on 4 March 2013).

43. Menth, M.; Hartmann, M.; Klein, D. Demo: Global Locator, Local Locator, and Identifier Split (GLI-Split). In Proceedings of the 9th Würzburg Workshop on IP: Visions of Future Generation Networks (EuroView), Würzburg, Germany, 27–28 July 2009.
44. Varga, A. INET Framework for the OMNeT++ Discrete Event Simulator. Available online: http://github.com/inet-framework/inet (accessed on 4 March 2013).
45. Varga, A.; Hornig, R. An Overview of the OMNeT++ Simulation Environment. In Proceedings of the International Conference on Simulation Tools and Techniques for Communications, Networks and Systems, Brussels, Belgium, 3–7 March 2008.
46. Bonaventure, O.; Filsfils, C.; Francois, P. Achieving Sub-50 milliseconds recovery upon BGP peering link failures. *IEEE/ACM Trans. Netw.* **2007**, *15*, 1123–1135.
47. Yamagata, I.; Shirasaki, Y.; Nakagawa, A.; Yamaguchi, J.; Ashida, H. NAT444 (Draft-Shirasaki-Nat444-06). Available online: http://tools.ietf.org/html/draft-shirasaki-nat444 (accessed on 4 March 2013).