Hierarchical IPv4 Framework

draft-frejborg-hipv4-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 24, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This draft describes a framework how the current IPv4 address structure can be extended towards a similar hierarchical numbering structure as used in the Public Switched Telephone Network and bring hierarchy to the routing architecture of Internet. The framework requires extensions to the existing Domain Name System architecture, the existing IPv4 stack of the end systems (hosts) and to routers in the Internet. The framework can be implemented incrementally to the hosts, databases and routers.

Table of Contents

1. Requirements Notation...........................................2
2. Introduction....................................................3
3. Definitions of Terms...........................................4
4. Extensions to Current Architectures..........................5
5. The header of a hIPv4 datagram................................7
6. Life of a hIPv4 Connection....................................8
7. Routing Policies of a RLOC Realm..............................10
8. Overlapping Source and Destination IP Addresses/Ports.......11
9. Traceroute Considerations....................................12
10. Multicast Considerations......................................12
11. Traffic Engineering Considerations..........................13
12. Large Encapsulated Packets...................................14
13. Mobility Considerations......................................14
14. Transition Considerations.....................................15
15. Security Considerations......................................15
16. IANA Considerations..........................................15
17. Conclusion....................................................15
18. References...................................................17
   18.1. References............................................17
   18.2. Informative References................................17
19. Acknowledgements............................................17

1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
2. Introduction

Today’s Internet flat routing architecture and single numbering addressing space has been discussed for several years, see [RFC4948]. A new address space (IPv6) has been developed but it will not change the flat routing architecture or the single numbering addressing space. The other global network, that is, the Public Switched Telephone Network (PSTN), have been build upon a hierarchical numbering architecture which have enabled a hierarchical signaling architecture. By using concepts and ideas from PSTN, Multiprotocol Label Switching (MPLS) and Locator/ID Separation Protocol [LISP] architectures, scaling benefits can be achieved. PSTN uses country- and national destination codes in the hierarchical numbering architecture, these codes can be considered similar as to the Routing Locator (RLOC) in [LISP]). The Endpoint Identifiers (EID) can be compared to Subscriber Numbers in PSTN. By using the RLOC and EID as a shim header (similar as in MPLS [RFC3032] and RBridge architectures [RBRIDGE]) a hierarchical addressing and routing architecture can be created.

Some of the design goals of this proposal include:

1. Minimize introduction of totally new protocols or signaling architectures, instead use well-proven established protocols and insert extension to protocols where needed.

2. Create a hierarchical routing architecture and therefore reduce the routing table size in the "default-free zone" (DFZ).

3. Remove IPv4 address block constraints; reuse IPv4 address blocks by a separator mechanism.

4. Improve site mobility, that is, a site wishes to changes its attachment point to the Internet without changing its IP address block.

5. Make use of the current forwarding plane (IPv4), introduce a new forwarding plane for only a few routers in an Autonomous System or service provider area.

6. Reduce the amount of Network Address Translation (NAT) demand for IPv4-to-IPv4 traffic.

7. Provide a smooth transition path from the current IPv4 framework to the hierarchical IPv4 framework.
3. Definitions of Terms

Regional Internet Registry (RIR)

is an organization overseeing the allocation and registration of Internet number resources within a particular region of the world. Resources include IP addresses (both IPv4 and IPv6) and autonomous system numbers.

Global RLOC Block (GRB)

an IPv4 address block that is globally unique.

Routing Locator (RLOC) Identifier:

an IPv4 address used in the LISP header allocated from the GRB and assigned by a RIR to a service provider or a multihomed enterprise with an Autonomous System (AS) number.

Endpoint Identifier (EID):

an IPv4 address used in the LISP header.

LISP header:

a 8 byte field consisting of RLOC and EID values

hIPv4 header:

A LISP header is inserted between the IPv4 header and the transport protocol, the new header combination is called a hIPv4 header.

LISP Switch Router (LSR):

A router capable to process the hIPv4 header; once the header is processed the LSR will forward the datagram upon the IPv4 destination address.

RLOC realm:

A RLOC realm can consist of one or several Autonomous System domains. A RLOC realm must have one attached LISP Switch Router, also a RLOC identifier must be assigned to the RLOC realm.

Provider Independent Address Space (PI-addresses):
an IPv4 address block that is assigned by a Regional Internet Registries directly to an end-user organization

Provider Aggregatable Address Space (PA-addresses):

an IPv4 address block assigned by a Regional Internet Registry to an Internet Service Provider which can be aggregated into a single route advertisement

4. Extensions to Current Architectures

A key concept is to preserve the amount of knowledge and applications that have been invested and deployed around the IPv4 protocol. By adding hierarchy to the routing architecture these investments can be preserved, a hierarchical routing architecture enables reuse of most of the already allocated IPv4 blocks. Because the hierarchical IPv4 framework is an evolution of the current IPv4 framework the transition can be applied incrementally.

To implement the hierarchical IPv4 framework some basic rules are needed:

1. The DNS architecture must support a new extension, that is, an A type Resource Record should be able to carry a RLOC identifier.

2. The hIPv4 capable host shall have information about the local RLOC identifier; the local RLOC identifier can be configured manually or provided via a new DHCP option.

3. A globally unique IPv4 address block shall be reserved; this block is called the Global RLOC Block (GRB). A service provider can have one or several host addresses allocated from the GRB. The GRB host address is the RLOC identifier for a service provider. A multihomed enterprise shall allocate a RLOC identifier from the GRB.

4. RLOC identifiers are announced via current BGP protocol to adjacent service providers and multihomed enterprises, the RLOC identifiers are installed in the RIB of the DFZ. When the hIPv4 framework is fully implemented only the GRB is announced between the service providers and multihomed enterprises. An area that only exchange GRB prefixes with other areas is called a RLOC realm.
5. A hIPv4 capable RLOC realm must have one or several LSRs attached to its realm. The RLOC identifier is configured as an Anycast IP address on the LSR. The Anycast IP address is installed to appropriate routing protocols in order to be distributed to the DFZ.

6. The IPv4 socket API at end hosts must be enhanced to support local and remote RLOC identifiers. The modified IPv4 socket API must be backward compatible with the current IPv4 socket API. The outgoing hIPv4 datagram must be assembled by the hIPv4 stack with the local IP address from the socket as the source IP address and the remote RLOC identifier as the destination IP address in the IPv4 header. The local RLOC identifier is inserted in the RLOC field of the LISP header. The remote IP address from the socket API is inserted in the EID field of the LISP header.

7. The hIPv4 datagram is routed upon the destination IPv4 address (that is, the remote RLOC identifier) towards the closest LSR configured with the remote RLOC identifier. When the LSR receives a hIPv4 datagram matching the local Anycast IP address, the LSR must swap the IPv4 and LISP header in order to reach the final destination inside the remote RLOC realm. The IPv4 address of the final destination is given in the EID field of the LISP header. When the swap is complete the final destination can be reached. You can say that the hIPv4 framework provides an AS destination based routing schema with IPv4 as the forwarding plane.

8. When the hierarchical routing architecture is fully implemented the global allocation of IP blocks is no longer valid. Instead a country or area based reservation of IPv4 blocks shall be developed. The new IP address allocation policy is out of scope in this document, only ideas are elaborated. For example, an enterprise shall be able to change its attachment point to Internet without renumbering of IP addresses - only RLOC identifier needs to be changed. Usually an enterprise has only a few attachments point to Internet and therefore there is no need to reserve a globally unique IP block. If an enterprise moves to another country it is acceptable that renumbering might be required.
5. The header of a hIPv4 datagram

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| IHL |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Routing Locator                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Endpoint ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The LISP header is inserted between the IP header and the transport protocol, that is, TCP or UDP. The LISP header consists of a Routing Locator field (4 bytes) and Endpoint ID field (4 bytes). In the current IPv4 framework, both TCP and UDP protocols calculate their header checksum values with the help of a pseudoheader. The pseudoheader calculation includes value from the IP header, that is, source IP address, destination IP address and value of the protocol field. By this mechanism more reliability is achieved.

To preserve current reliability level the hIPv4 stack shall also include the RLOC and EID values when calculation of the TCP and UDP pseudoheader is applied. Therefore, a mechanism to identify when to include RLOC and EID values in the pseudoheader calculation is needed.

When the hIPv4 stack is assembling the datagram for transport the hIPv4 stack shall decide if a legacy IPv4 or hIPv4 header is used upon RLOC information. If the local RLOC equals the remote RLOC value there is no need to use the hIPv4 header; datagram is routed upon the IPv4 header since the datagram will not exit the local RLOC realm. But when the local RLOC identifier doesn’t match the remote RLOC identifier a hIPv4 header must be assembled because the datagram must be routed to a remote RLOC realm. TCP and UDP pseudoheader checksum calculation shall be extended to include RLOC and EID values. Because
routers and hosts are still using the IPv4 framework the devices must detect when a hIPv4 header is used. IPv4 uses protocol values for TCP, UDP, ICMP, GRE, IP-in-IP and so on. It is recommended that new values are reserved for the current IPv4 protocols in the hIPv4 framework. The new protocol values will act as an indicator of the usage of the hIPv4 header. The IPv4 socket API will not be aware of the new protocol values; it is the hIPv4 stack at the client that changes the protocol value when a remote RLOC realm connection is established. When the datagram has reached the server the hIPv4 stack changes the protocol value to the appropriate IPv4 value for the socket API. Therefore the application is not aware of new protocol values.

6. Life of a hIPv4 Connection

This section provides an example of a hIPv4 connection between two IPv4 hosts; a client and a server residing in different RLOC realms.

1. The client queries the DNS server; the hIPv4 stack notice that the local and remote RLOC doesn’t match and therefore must use the hIPv4 header for the connection. The hIPv4 socket of the client must assemble the datagram in the following way:

   a. change the protocol value to match appropriate hIPv4 value
   b. local IP address from API -> source IP address
   c. remote IP address from API -> EID field
   d. local RLOC identifier -> RLOC field
   e. remote RLOC identifier-> destination IP address

2. Apply checksum calculations, include RLOC and EID values for the pseudoheader calculation, when completed the datagram is transmitted.

3. The hIPv4 datagram is routed throughout Internet upon the destination IP address of the IPv4 header.

4. The hIPv4 datagram will reach the closest LSR of the remote RLOC realm. When the LSR notice that the datagram matches the given local RLOC value the LSR must:
a. verify IP and TCP/UDP checksums, include RLOC and EID values for the pseudoheader calculation

b. replace the source address in the IPv4 header with the RLOC value of the LISP header

c. replace the destination address in the IPv4 header with the EID value of the LISP header

d. replace the RLOC value in the LISP header with the destination IP address of the IPv4 header

e. replace the EID value in the LISP header with the source IP address of the IPv4 header

f. decrease TTL with one

g. calculate IP and TCP/UDP checksums, include RLOC and EID values for the pseudoheader calculation

h. forward the datagram upon the destination IP address of the IPv4 header

5. The swapped hIPv4 packet is now routed inside the remote RLOC realm upon the new destination IP address of the IPv4 header to the final destination.

6. The server receives the hIPv4 datagram, the hIPv4 stack must verify IP and TCP/UDP checksums, include RLOC and EID values for the pseudoheader calculation

7. The hIPv4 stack of the server must present to the IPv4 socket API the following:

   a. change the protocol value to match appropriate IPv4 value

   b. source IP address -> remote RLOC identifier

   c. destination IP address -> local IP address

   d. RLOC -> local RLOC

   e. EID -> remote IP address
8. The server’s application will respond to the client and the returning datagram will take the almost the same steps, that is step 1 to 6, as when the client started the session. In step 1 the server doesn’t need to do a DNS lookup since all information is provided by the datagram.

7. Routing Policies of a RLOC Realm

This section is not part of the draft, it is used to discuss and study how the hIPv4 framework could influence on the IPv4 address allocation and routing policies to ensure that the framework will enable some re-usage of IPv4 address blocks. It is the Regional Internet Registries (RIRs) that shall define the final policies.

When the hIPv4 framework is fully implemented every RLOC realm can have a full IPv4 address space - except the GRB - to allocate IPv4 address blocks from. There are some implications though. In order for an enterprise to achieve site mobility, that is, to change service provider without changing its IP addressing schema, the enterprise should implement an Autonomous System (AS) solution with RLOC identifier at the attachment point to the service provider. Larger enterprises do have the resources to implement AS border routing; most of the large enterprises have already implemented multihoming solutions. The small and midsize enterprises (SME) may not have the resources to implement AS border routing, or the implementation introduces unnecessary costs for the SME. Also if every SME needs to have a RLOC identifier it will have an impact on the RIB at the DFZ, the RIB will be populated with a huge amount of RLOC prefixes.

It is clear that a compromise is needed. A SME is usually single-homed and the SME should be able to reserve a PI address block from the RIR without the need to be forced to use a RLOC realm solutions, that is, implement LSR and AS border routing. The PI address block is no longer globally unique, the SME can only reserve the PI address block for the country or countries where it is active or has it attachment point to Internet. The attachment point rarely changes to another country; therefore it is sufficient that the PI address block is locally unique. When the SME is replacing its Internet service provider the SME do not have to change its IPv4 addressing schema - only the local RLOC identifier at the hosts are changed. The internal traffic at an SME does not use the RLOC identifier, the internal routing is applied by the IPv4 header and thus the internal routing and addressing architectures are preserved.

Mergers and acquisitions of SME can cause IP address conflicts, because the PI address block is hereafter only locally unique. If a SME in country A overtakes a SME in country B there is a slight
chance that both SME can have overlapping IPv4 addresses. An idea to address this scenario is to categorize the SME upon their business areas. It is highly unlikely that a SME in, for example, agriculture business area will ever acquire a SME in the medical business area, or vice versa. When a SME applies for a PI address block the RIR could verify to which business area the SME operates in and do a global check in order to give the SME a globally unique IP address block from that business area. Large enterprises also merge, but since the large enterprises are usually multihomed the merger of networks can be rapidly carried out with the help of RLOC realm routing. During a merger usually the infrastructure of a company is slowly incorporated to the other company’s infrastructure, this integration usually requires redesign of the network architecture and therefore in most cases the RLOC realm routing can be removed.

Finally, residential users will receive only PA addresses. When a residential user changes a service provider the residential user has to replace the IP addresses. A PA IP address block is no longer globally unique, every Internet service provider can use the PA address blocks at their RLOC realms.

The hIPv4 framework will provide re-usage of IPv4 address blocks, the globally unique reservation of IPv4 address block shall be replaced by a country or area specific allocation. The biggest challenge is when merger and acquisitions are carried out, there is chance that overlapping of IP addresses could still happen but the hIPv4 framework reduces this problem to a minimum compared what is seen today during mergers with the usage of private IP addresses [RFC1918].

8. Overlapping Source and Destination IP Addresses/Ports

Since source and destination IPv4 addresses are only locally significant within a RLOC realm there is a slight chance that connections between RLOC realms with similar source and destination IP addresses could be established. But the connection is still unique because two processes communicating over TCP form a logical connection that is uniquely identifiable by the tuplets involved, that is by the combination of <local_IP_address, local_port, remote IP address, remote port>.

The connection could be no longer unique when two clients with the same source IP address in different RLOC realms are accessing a server locate in a third RLOC realm. In this scenario a chance exists that the clients will use the same local port value. This situation will cause an "identical connection situation" for the application layer. To overcome this scenario the hIPv4 stack must accept only one
unique connection with the help of the RLOC information. If there is an "identical connection situation" - that is, both clients uses the same values in the tuplets <local_IP_address, local_port, remote_IP_address, remote_port> - the hIPv4 stack shall allow only the first established connection to continue, the following connections must be prohibited and the clients are informed by ICMP notification about the "identical connection situation".

9. Traceroute Considerations

As long as the traceroute is executed inside the RLOC realm normal IPv4 traceroute mechanism can be used. As soon as the traceroute exits the originating RLOC realm the LISP header shall be used in the notifications. Therefore extension to ICMP protocol shall be implemented, the extensions shall be compatible with [RFC4884].

10. Multicast Considerations

Since source and destination IPv4 prefixes are only installed in the RIB of the local RLOC realm there is a constraint with Reverse Path Forwarding (RPF) which is used to ensure loop-free forwarding of multicast packets. The source IP address of a multicast group (S,G) is used against the RFP check. The source IP address can no longer be used as a RFP checkpoint outside the local RLOC realm.

To enable RPF globally for a (S,G), the multicast enabled LSR (mLSR) must at the source RLOC realm replace the source IP address with the local RLOC identifier for inter-RLOC multicast streams. This can be achieved if the local LSR act also as an Anycast Rendezvous Point with Multicast Source Discovery Protocol (MSDP) capabilities; with these functionalities the LSR becomes a multicast enabled LSR (mLSR). The sender register at the mLSR and a source tree is established between the sender and the mLSR. When an inter-RLOC realm receiver subscribes to the multicast group the mLSR have to swap the IPv4 multicast datagram in the following way:

   a. verify IP and UDP checksums, include RLOC and EID values for the pseudoheader calculation
   b. source IP address -> local RLOC
   c. destination IP address : no changes
   d. RLOC : no changes
   e. EID : no changes
f. decrease TTL with one

g. calculate IP and UDP checksums, include RLOC and EID values for the pseudoheader calculation

h. forward the datagram to the shared multicast tree

In order for the mLSR to function as described above the sender must assemble the multicast hIPv4 datagram in the following way:

a. change the protocol value to match appropriate hIPv4 value

b. local IP address from API -> source IP address (S) -> EID

c. remote IP address from API -> destination IP address (G)

d. local RLOC -> RLOC

e. remote RLOC : not applicable

The downstream routers from the mLSR to the receiver will use the source IP address in the IPv4 header for RPF verification. In order for the receiver to create RTCP receiver reports all information is provided in the hIPv4 header of the datagram.

Since Source Specific Multicast (SSM) schema is a raw socket application, SSM will need an extension; RLOC and EID extensions shall be added to SSM.

11. Traffic Engineering Considerations

When hIPv4 framework is fully implemented ingress load balancing to a RLOC realm can be influenced by the placement of LSRs at the realm; a LSR provides "nearest routing" schema. Also, if RIR policies allows, a service provider can have several RLOC assigned, hence traffic engineering and filtering can be done with the help of RLOC identifiers. Sensitive traffic can be aggregated under one RLOC identifier which is not fully distributed into the DFZ of Internet.

If needed an RLOC Traffic Engineering solution between RLOC realms might be developed, that is, create explicit paths that can be engineered via specific RLOC identifiers. Further studies are needed; first it should be evaluated if there is demand for such a solution.
12. Large Encapsulated Packets

Adding the LISP header to an IPv4 datagram in order to create a hIPv4 datagram will increase the size of it but since the datagram is assembled at the host it will not add complications of current Path MTU Discovery (PMTUD) mechanism in the network. The intermediate network between two hosts will not see any difference in the size of datagram; IPv4 and hIPv4 datagram sizes are the same from the network point of view.

13. Mobility Considerations

This document will consider two types of mobility solutions, site mobility and host mobility.

Site mobility definition:

a site wishes to changes its attachment point to the Internet without changing its IP address block

Today multihoming is the only solution for enterprises that wishes to achieve site mobility. Multihoming is one of the key findings behind the growth of the DFZ, see [RFC4948], sections 2.1 and 3.1.2. The hIPv4 framework can provide a solution for enterprises to have site mobility without the requirement of implementing a multihomed solution. This singlehomed solution with PI addresses is discussed in section 7. When a singlehomed enterprise changes it attachment points to the Internet the IP address structure remains intact but RLOC identifier needs to be replaced.

Host mobility definition:

a host moves relatively rapidly between different networks, changing its IP layer network attachment point

Mobile IP [RFC3344bis] is used today for IPv4 hosts in order to provide mobility. Mobile IP is an overlay protocol; it is also a raw socket application that uses IP addresses in its architecture. It is obvious that hIPv4 extensions are needed to achieve a Mobile IP solution when the hIPv4 headers are used. But Mobile IP is not the only solution offering mobility for hosts, studies has been carried out on how mobility could be achieved by improving the IPv4 stack. These solutions are not widely known. One major benefit by adding a "mobile extension" to the IPv4 stack is that we can remove the overlay architecture. Because hIPv4 framework requires changes to the current IPv4 stack it should be investigate if the studies of "An
End-to-End Approach to Host Mobility" [E2EHM] and "Reliable Network Connections" [RNC] can be integrated to the hIPv4 stack.

14. Transition Considerations

The hIPv4 framework is not introducing a complete new protocol; it imposes extensions to the current IPv4 stack, databases and to some raw socket protocols but the current forwarding plane at the Internet remains intact apart from that a few new router element (the LSR) is needed at each RLOC realm. Extensions to the IPv4 stack, databases, raw socket applications and routers can be deployed in parallel. Even genuine hIPv4 connections can be established between hosts though the current flat Internet structure is still present. When will then the flat routing architecture be removed? The author thinks there are two possible tipping points:

- when the RIB of DFZ is getting close to the capabilities of current forwarding plane - who will pay for the upgrade? Or will the service provider only accept GRB prefixes from other service providers and avoid capital expenses?
- when the exhaust of IPv4 addresses is causing enough problems for enterprises

The enterprises and Internet service providers have a relationship, both also have a common interest that Internet is available and affordable - these factors will drive the evolution towards the hIPv4 framework. And the IPv4 framework will not be abandoned; it will be still used inside a RLOC realm.

15. Security Considerations

Hijacking of a single prefix by longest match from another RLOC realm is no longer possible since the prefixes are separated by a locator, the RLOC identifier. To apply a highjack of a certain prefix the whole RLOC realm must be routed via a bogus RLOC realm. Studies should be carried out with the Secure Inter-Domain Routing (SIDR) workgroup if the RLOC identifiers can be protected from hijacking.

16. IANA Considerations

TBD

17. Conclusion

This document gives a high level overview of the hierarchical IPv4 framework which could be build in parallel with the current flat
Internet by implementing extensions at several architectures. Implementation of the hIPv4 framework will not require a major service window break in the Internet, neither at the internal networks of enterprises. Basically, the hIPv4 framework is an evolution of the current IPv4 framework. For connections inside a RLOC realm the IPv4 framework will be used in the future and for inter-RLOC realm communications the hIPv4 framework is needed.

Raw socket applications, such as for example SIP and IPsec will need major modifications in order to be able to utilize the hIPv4 framework.
18. References

18.1. References


18.2. Informative References


[RBRIDGE] Perlman, R., "RBridges, Transparent Routing", Infocomm, 2004


[RNC] Zandy, V.C., Miller, B.P., "Reliable Network Connections", Computer Sciences Department University of Wisconsin, 2002

19. Acknowledgements

The author would like to acknowledge Aki Anttila for giving helpful feedback.
Authors’ Addresses

Patrick Frejborg
Consultant

Email: pfrejborg@gmail.com