

Softwires Working Group
Internet-Draft
Intended status: Informational
Expires: May 17, 2013

M. Boucadair, Ed.
France Telecom
S. Matsushima
Softbank Telecom
Y. Lee
Comcast
O. Bonness
Deutsche Telekom
I. Borges
Portugal Telecom
G. Chen
China Mobile
November 13, 2012

Motivations for Carrier-side Stateless IPv4 over IPv6 Migration
Solutions
draft-ietf-softwire-stateless-4v6-motivation-05

Abstract

IPv4 service continuity is one of the most pressing problems that must be resolved by Service Providers during the IPv6 transition period – especially after the exhaustion of the public IPv4 address space. Current standardization effort that addresses IPv4 service continuity focuses on stateful mechanisms. This document elaborates on the motivations for the need to undertake a companion effort to specify stateless IPv4 over IPv6 approaches.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on May 17, 2013.

Copyright Notice

Internet-Draft

Solution Motivations

November 2012

Copyright (c) 2012 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	Why Stateless IPv4 over IPv6 Solutions are Needed?	4
3.1.	Network Architecture Simplification	4
3.1.1.	Network Dimensioning	4
3.1.2.	No Intra-domain Constraint	5
3.1.3.	Logging - No Need for Dynamic Binding Notifications .	5
3.1.4.	No Additional Protocol for Port Control is Required .	5
3.2.	Operational Tasks and Network Maintenance Efficiency . . .	6
3.2.1.	Preserve Current Practices	6
3.2.2.	Planned Maintenance Operations	6
3.2.3.	Reliability and Robustness	6
3.2.4.	Support of Multi-Vendor Redundancy	6
3.2.5.	Simplification of Qualification Procedures	7
3.3.	Facilitating Service Evolution	7
3.3.1.	Implicit Host Identification	7
3.3.2.	No Organizational Impact	8
3.4.	Cost Minimization Opportunities	8
4.	Discussion	9
4.1.	Dependency Between IPv4 and IPv6 Address Assignments . . .	10
4.2.	IPv4 Port Utilisation Efficiency	10
4.3.	IPv4 Port Randomization	11
5.	Conclusion	11
6.	IANA Considerations	11
7.	Security Considerations	11
8.	Contributors	12
9.	Acknowledgments	12

10. Informative References	12
Authors' Addresses	14

[1.](#) Introduction

When the global IPv4 address space is exhausted, Service Providers will be left with an address pool that cannot be increased anymore. Many services and network scenarios will be impacted by the lack of IPv4 public addresses. Providing access to the (still limited) IPv6 Internet only won't be sufficient to address the needs of customers, as most of them will continue to access legacy IPv4-only services. Service Providers must guarantee their customers that they can still access IPv4 contents although they will not be provisioned with a global IPv4 address anymore. Means to share IPv4 public addresses are unavoidable [[RFC6269](#)].

Identifying the most appropriate solution(s) to the IPv4 address exhaustion as well as IPv4 service continuity problems and deploying them in a real network with real customers is a very challenging and complex process for all Service Providers. There is no one size fits all solution. Each Service Provider has to take into account its own context (e.g., service infrastructures), policies and marketing strategy (a document that informs Service Providers about the impact of the IPv4 address shortage, and provides some recommendations and guidelines, is available at [[EURESCOM](#)]).

Current standardization efforts to address the IPv4 service continuity issue focuses on stateful mechanisms that share global IPv4 addresses between customers with NAT (Network Address Translation) capabilities in the network. Because of some caveats of such stateful approaches, the Service Provider community feels that a companion effort is required to specify stateless IPv4 over IPv6 approaches. In the context of address sharing, states should be maintained in other equipments, e.g. customer premises equipment or host.

This document focuses on carrier-side stateless IPv4 over IPv6.

More discussions about stateless vs. stateful can be found at

[\[RFC6144\]](#).

2. Terminology

This document makes use of the following terms:

State: as used in [\[RFC1958\]](#).

Session state: refers to an information state as defined in [Section 2.3 of \[RFC2663\]](#). In particular, it refers to the state maintained by the NAT so that datagrams pertaining to a session are routed to the right node. Note, TCP/UDP sessions are uniquely identified by the tuple of (source IP address, source TCP/UDP port, target IP address, target TCP/UDP port) while ICMP query sessions are identified by the tuple of (source IP address, ICMP query ID, target IP address).

User-session state: refers to session state belonging to a given user.

Stateful 4/6 solution (or stateful solution in short): denotes a solution where a NAT in the Service Provider's network maintains user-session states [\[I-D.ietf-behave-lsn-requirements\]](#). The NAT function is responsible for sharing the same IPv4 address among several subscribers and for maintaining user-session state.

Stateless 4/6 solution (or stateless solution in short): denotes a solution which does not require any per-user state (see [Section 2.3 of \[RFC1958\]](#)) to be maintained by any IP address sharing function in the Service Provider's network. A dependency between an IPv6 prefix and IPv4 address is assumed. In an IPv4 address sharing context, dedicated functions are enabled in the CPE router to restrict the source IPv4 port numbers. Within this document, "port set" and "port range" terms are used interchangeably.

[3.](#) Why Stateless IPv4 over IPv6 Solutions are Needed?

The following sub-sections discuss different aspects that motivate this effort.

[3.1.](#) Network Architecture Simplification

The activation of the stateless function in the Service Provider's network does not introduce any major constraint on the network architecture and its engineering. The following sub-sections elaborate on these aspects.

[3.1.1.](#) Network Dimensioning

Because no per-user state [[RFC1958](#)] is required, a stateless solution does not need to take into account the maximum number of simultaneous user-sessions and the maximum number of new user-sessions per second to dimension its networking equipment. Like current network dimensioning practices, only considerations related to the customers

number, traffic trends and the bandwidth usage need be taken into account.

[3.1.2.](#) No Intra-domain Constraint

Stateless IPv4/IPv6 interconnection functions can be ideally located at the boundaries of an Autonomous System (e.g., Autonomous System Border Routers (ASBRs) that peer with external IPv4 domains); in such case intra-domain paths are not altered: there is no need to force IP packets to cross a given node for instance; intra-domain routing processes are not tweaked to direct the traffic to dedicated nodes. Stateless solutions optimize CPE-to-CPE communication in that packets don't go through the interconnection function.

[3.1.3.](#) Logging – No Need for Dynamic Binding Notifications

Network abuse reporting requires traceability [[RFC6269](#)]. To provide such traceability, prior to IPv4 address sharing, logging the IPv4 address assigned to a user was sufficient and generates relatively small logs. The advent of stateful IPv4 address allows dynamic port assignment, which then requires port assignment logging. This logging of port assignments can be considerable.

In contrast, static port assignments do not require such considerable logging. The volume of the logging file may not be seen as an important criterion for privileging a stateless approach because stateful approaches can also be configured (or designed) to assign port ranges and therefore lead to acceptable log volumes.

If a dynamic port assignment mode is used, dedicated interfaces and protocols must be supported to forward binding data records towards dedicated platforms. The activation of these dynamic notifications may impact the performance of the dedicated device. For stateless solutions, there is no need for dynamic procedures (e.g., using SYSLOG) to notify a mediation platform about assigned bindings.

Some Service Providers have a requirement to use only existing logging systems and to avoid introducing new ones (mainly because of Capital Expenditure (CAPEX) considerations). This requirement is easily met with stateless solutions.

3.1.4. No Additional Protocol for Port Control is Required

Stateless solutions do not require activating a new dynamic signaling protocol in the end-user CPE in addition to those already used. In particular, existing protocols (e.g., UPnP IGD:2 [[UPnP-IGD](#)]) can be used to control the NAT mappings in the CPE.

Note: To overcome some security concerns, IGD:2 authorization framework [[UPnP-IGD](#)] should be used and security considerations elaborated in [[Sec_DCP](#)] should be taken into account.

3.2. Operational Tasks and Network Maintenance Efficiency

3.2.1. Preserve Current Practices

If stateless solutions are deployed, common practices are preserved. In particular, the maintenance and operation of the network do not require any additional constraints such as: path optimization practices, enforcing traffic engineering policies, issues related to traffic oscillation between stateful devices, load-balancing the traffic or load sharing the traffic among egress/ingress points can be used, etc. Particularly,

- o anycast-based schemes can be used for load-balancing and redundancy purposes between nodes embedding the Stateless IPv4/IPv6 interconnection function.
- o asymmetric routing to/from the IPv4 Internet is natively supported and no path-pinning mechanisms have to be additionally implemented.

[3.2.2.](#) Planned Maintenance Operations

Since no state is maintained by stateless IPv4/IPv6 interconnection nodes, no additional constraint needs to be taken into account when upgrading these nodes (e.g., adding a new service card, upgrading hardware, periodic reboot of the devices, etc.). In particular, current practices that are enforced to (gracefully) reboot or to shutdown routers can be maintained.

[3.2.3.](#) Reliability and Robustness

Compared to current practices (i.e., without a Carrier Grade NAT (CGN) in place), no additional capabilities are required to ensure reliability and robustness in the context of stateless solutions. Since no state is maintained in the Service Provider's network, state synchronization procedures are not required.

High availability (including failure recovery) is ensured owing to best current practices in the field.

[3.2.4.](#) Support of Multi-Vendor Redundancy

Deploying stateful techniques, especially when used in the Service Providers networks, constrains severely deploying multi-vendor

redundancy since very often proprietary vendor-specific protocols are used to synchronize state. This is not an issue for the stateless case. Concretely, the activation of the stateless IPv4/IPv6 interconnection function does not prevent nor complicate deploying devices from different vendors.

This criterion is very important for Service Providers because they want to avoid being locked into one vendor for their entire network

and they want to operate multi-vendor-supplied networks.

3.2.5. Simplification of Qualification Procedures

The introduction of new functions and nodes into operational networks follows strict procedures elaborated by Service Providers. These procedures include in-lab testing and field trials. Because of their nature, stateless implementations optimize testing time and procedures:

- o The specification of test suites to be conducted should be shorter;
- o The required testing resources (in terms of manpower) are likely to be less solicited than they are for stateful approaches.

One of the privileged approaches to integrate stateless IPv4/IPv6 interconnection function consists in embedding stateless capabilities in existing operational nodes (e.g., IP router). In this case, any software or hardware update would require to execute non-regression testing activities. In the context of the stateless solutions, the non-regression testing load due to an update of the stateless code is expected to be minimal.

For the stateless case, testing effort and non-regression testing are to be taken into account for the CPE side. This effort is likely to be lightweight compared to the testing effort, including the non-regression testing, of a stateful function which is co-located with other routing functions for instance.

3.3. Facilitating Service Evolution

3.3.1. Implicit Host Identification

Service Providers do not offer only IP connectivity services but also added value services (a.k.a., internal services). Upgrading these services to be IPv6-enabled is not sufficient because of legacy devices. In some deployments, the delivery of these added-value services relies on implicit identification mechanism based on the source IPv4 address. Due to address sharing, implicit identification

will fail [[RFC6269](#)]; replacing implicit identification with explicit

authentication will be seen as a non acceptable service regression by the end users (less Quality of Experience (QoE); refer to [Section 4.2 \[RFC6462\]](#)).

When a stateless solution is deployed, implicit identification for internal services is likely to be easier to implement: the implicit identification should be updated to take into account the port range and the IPv4 address. Techniques as those analyzed in [\[I-D.ietf-intarea-nat-reveal-analysis\]](#) are not required for the delivery of these internal services if a stateless solution is deployed.

Note stateful approaches configured to assign port ranges allow also to support implicit host identification.

[3.3.2.](#) No Organizational Impact

Stateless solutions adopt a clear separation between the IP/transport layers and the service layers; no service interference is to be observed when a stateless solution is deployed. This clear separation:

Facilitates service evolution: Stateless solutions admit applications which can be deployed without enabling any application-specific function (e.g., Application Level Gateway (ALG)) in the Service Provider's network. Avoiding ALGs is highly desirable.

Limits vendor dependency: The upgrade of value-added services does not involve any particular action from vendors that provide devices embedding the stateless IPv4/IPv6 interconnection function.

No service-related skills are required for network operators who manage devices that embed the IPv4/IPv6 interconnection function: IP teams can be in charge of these devices; there is a priori no need to create a dedicated team to manage and to operate devices embedding the stateless IPv4/IPv6 interconnection function. The introduction of stateless capabilities in the network are unlikely to degrade management costs.

[3.4.](#) Cost Minimization Opportunities

To make decision for which solution is to be adopted, Service Providers usually undertake comparative studies about viable technical solutions. It is not only about technical aspects but also economical optimization (both CAPEX and Operational Expenditure

(OPEX) considerations). From a Service Provider perspective, stateless solutions may be more attractive because it impacts the current network operations and maintenance model less than stateful solutions. Table 1 shows the general correspondence between technical benefits and potential economic reduction opportunities.

While not all Service Providers environments are the same, a detailed case study from one Service Provider [[I-D.matsushima-v6ops-transition-experience](#)] reports that stateless transition solutions can be considerably less expensive than stateful transition solutions.

Section	Technical and Operation Benefit	Cost Area
Section 3.1.1	Network dimensioning	Network
Section 3.1.2	No Intra-domain constraint	Network
Section 3.1.3	Logging	Network & Ops
Section 3.1.4	No additional control protocol	Network
Section 3.2.1	Preserve current practices	Ops
Section 3.2.2	Planned maintenance	Ops
Section 3.2.3	Reliability and robustness	Network & Ops
Section 3.2.4	Multi-Vendor Redundancy	Network
Section 3.2.5	Simple qualification	Ops
Section 3.3.1	Implicit Host Identification for internal services	Ops
Section 3.3.2	Organizational Impact	Ops

Table 1: Cost minimization considerations

[4.](#) Discussion

Issues common to all address sharing solutions are documented in [\[RFC6269\]](#). The following sub-sections enumerate some open questions

for a CPE-based stateless solution. There are no universal answers to these open questions since each Service Provider has its own constraints (e.g., available address pool, address sharing ratio, etc.).

[4.1.](#) Dependency Between IPv4 and IPv6 Address Assignments

Complete stateless mapping implies that the IPv4 address and the significant bits that are used to encode the set of assigned ports can be retrieved from the IPv6 prefix assigned to the CPE. This requirement can be addressed by either using the IPv6 prefix also used to forward IPv6 traffic natively, or allocating two prefixes to the CPE (one that will be used to forward IPv6 traffic natively, and the other one to forward IPv4 traffic).

- o Providing two IPv6 prefixes avoids the complexity that may be related to the adaptation of the IPv6 addressing scheme to the IPv4 addressing scheme. The drawback is the need to allocate two prefixes instead of one to each CPE and to announce them accordingly, possibly at the cost of jeopardizing the routing and forwarding efficiencies.
- o The use of a single prefix to cover both the forwarding of IPv6 and IPv4-in-IPv6 traffic avoids the need to maintain a double information (e.g., for customer identification and management purposes and for forwarding table maintenance purposes). This scheme somewhat links strongly the IPv4 addressing scheme to the allocated IPv6 prefixes. For Service Providers requiring to apply specific policies on per Address-Family (e.g., IPv4, IPv6), some provisioning tools (e.g., DHCPv6 option) may be required to derive in a deterministic way the IPv6 address to be used for the IPv4 traffic based on the IPv6 prefix delegated to the home network.

[4.2.](#) IPv4 Port Utilisation Efficiency

CGN-based solutions, because they can dynamically assign ports, provide better IPv4 address sharing ratio than stateless solutions (i.e., can share the same IP address among a larger number of customers). For Service Providers who desire an aggressive IPv4

address sharing, a CGN-based solution is more suitable than the stateless. However

- 1: When port overloading is used, some applications are likely to be broken.

- 2: in case a CGN pre-allocates port ranges, e.g.- to alleviate traceability complexity (see [Section 3.1.3](#)), it also reduces its port utilization efficiency.

[4.3.](#) IPv4 Port Randomization

Preserving port randomization [[RFC6056](#)] may be more or less difficult depending on the address sharing ratio (i.e., the size of the port space assigned to a CPE). The CPE can only randomize the ports inside a fixed port range.

More discussion to improve the robustness of TCP against Blind In-Window Attacks can be found at [[RFC5961](#)]. Other means than the (IPv4) source port randomization to provide protection against attacks should be used (e.g., use [[I-D.vixie-dnsextdns0x20](#)] to protect against DNS attacks, [[RFC5961](#)] to improve the robustness of TCP against Blind In-Window Attacks, use IPv6).

[5.](#) Conclusion

As discussed in [Section 3](#), stateless solutions provide several interesting features. Trade-off between the positive vs. negative aspects of stateless solutions is left to Service Providers. Each Service Provider will have to select the appropriate solution (stateless, stateful or even both) meeting its requirements.

This document recommends to undertake as soon as possible the appropriate standardization effort to specify a stateless IPv4 over IPv6 solution.

6. IANA Considerations

No action is required from IANA.

7. Security Considerations

Except for the less efficient port randomization of and routing loops [[RFC6324](#)], stateless 4/6 solutions are expected to introduce no more security vulnerabilities than stateful ones. Because of their stateless nature, they may in addition reduce denial of service opportunities.

Boucadair, et al.

Expires May 17, 2013

[Page 11]

Internet-Draft

Solution Motivations

November 2012

8. Contributors

The following individuals have contributed to this document:

Christian Jacquenet
France Telecom
Email: christian.jacquenet@orange.com

Pierre Levis
France Telecom
Email: pierre.levis@orange.com

Masato Yamanishi
SoftBank BB
Email: myamanis@bb.softbank.co.jp

Yuji Yamazaki
Softbank Mobile
Email: yuyamaza@bb.softbank.co.jp

Hui Deng
China Mobile
Email: denghui02@gmail.com

9. Acknowledgments

Many thanks to the following individuals who provided valuable comments:

X. Deng	W. Dec	D. Wing	A. Baudot
E. Burgey	L. Cittadini	R. Despres	J. Zorz
M. Townsley	L. Meillarec	R. Maglione	J. Queiroz
C. Xie	X. Li	O. Troan	J. Qin
B. Sarikaya	N. Skoberne	J. Arkko	D. Lui

10. Informative References

[EURESCOM]

Levis, P., Borges, I., Bonness, O. and L. Dillon L., "IPv4 address exhaustion: Issues and Solutions for Service Providers", March 2010, <<http://archive.eurescom.eu/~pub/deliverables/documents/P1900-series/P1952/D2bis/P1952-D2bis.pdf>>.

Boucadair, et al.

Expires May 17, 2013

[Page 12]

Internet-Draft

Solution Motivations

November 2012

[I-D.ietf-behave-lsn-requirements]

Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", [draft-ietf-behave-lsn-requirements-09](#) (work in progress), August 2012.

[I-D.ietf-intarea-nat-reveal-analysis]

Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments", [draft-ietf-intarea-nat-reveal-analysis-04](#) (work in progress), August 2012.

[I-D.matsushima-v6ops-transition-experience]

Matsushima, S., Yamazaki, Y., Sun, C., Yamanishi, M., and J. Jiao, "Use case and consideration experiences of IPv4 to IPv6 transition", [draft-matsushima-v6ops-transition-experience-02](#) (work in progress), August 2012.

progress), March 2011.

[I-D.vixie-dnsexp-dns0x20]

Vixie, P. and D. Dagon, "Use of Bit 0x20 in DNS Labels to Improve Transaction Identity", [draft-vixie-dnsexp-dns0x20-00](#) (work in progress), March 2008.

[RFC1958] Carpenter, B., "Architectural Principles of the Internet", [RFC 1958](#), June 1996.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", [RFC 2663](#), August 1999.

[RFC5961] Ramaiah, A., Stewart, R., and M. Dalal, "Improving TCP's Robustness to Blind In-Window Attacks", [RFC 5961](#), August 2010.

[RFC6056] Larsen, M. and F. Gont, "Recommendations for Transport-Protocol Port Randomization", [BCP 156](#), [RFC 6056](#), January 2011.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", [RFC 6144](#), April 2011.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", [RFC 6269](#), June 2011.

Boucadair, et al.

Expires May 17, 2013

[Page 13]

Internet-Draft

Solution Motivations

November 2012

[RFC6324] Nakibly, G. and F. Templin, "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", [RFC 6324](#), August 2011.

[RFC6462] Cooper, A., "Report from the Internet Privacy Workshop", [RFC 6462](#), January 2012.

[Sec_DCP] UPnP Forum, "Device Protection:1", November 2009.

[UPnP-IGD]

UPnP Forum, "Universal Plug and Play (UPnP) Internet

Gateway Device (IGD) V 2.0", December 2010,
<<http://upnp.org/specs/gw/igd2/>>.

Authors' Addresses

Mohamed Boucadair (editor)
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange.com

Satoru Matsushima
Softbank Telecom
Tokyo
Japan

Email: satoru.matsushima@tm.softbank.co.jp

Yiu Lee
Comcast
US

Email: Yiu_Lee@Cable.Comcast.com

Olaf Bonness
Deutsche Telekom
Germany

Email: Olaf.Bonness@telekom.de

Isabel Borges
Portugal Telecom
Portugal

Email: Isabel@ptinovacao.pt

Gang Chen
China Mobile
53A,Xibianmennei Ave.
Beijing, Xuanwu District 100053
China

Email: chengang@chinamobile.com