

Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 11, 2011

M. Boucadair, Ed.
France Telecom
S. Matsushima
Softbank Telecom
Y. Lee
Comcast
O. Bonness
Deutsche Telekom
I. Borges
Portugal Telecom
G. Chen
China Mobile
June 9, 2011

Motivations for Stateless IPv4 over IPv6 Migration Solutions
draft-operators-softwire-stateless-4v6-motivation-02

Abstract

IPv4 service continuity is one of the most sensitive 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 December 11, 2011.

Copyright Notice

Copyright (c) 2011 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	4
3. Why Stateless IPv4 over IPv6 Solutions are Needed?	5
3.1. Network Architecture Simplification	5
3.1.1. Network Dimensioning	5
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	6
3.1.5. Bandwidth Saving	6
3.2. Operational Tasks and Network Maintenance Efficiency	6
3.2.1. Preserve Current Practices	6
3.2.2. Planned Maintenance Operations	7
3.2.3. Reliability and Robustness	7
3.2.4. Support of Multi-Vendor Redundancy	7
3.2.5. Simplification of Qualification Procedures	7
3.3. Facilitating Service Evolution	8
3.3.1. Implicit Host Identification	8
3.3.2. No Organizational Impact	9
3.4. Cost Minimization Opportunities	9
4. Conclusion	10
5. IANA Considerations	10
6. Security Considerations	11
7. Contributors	11
8. Acknowledgments	11
9. Informative References	12
Authors' Addresses	13

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 [I-D.ietf-intarea-shared-addressing-issues].

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 nothing like a "One size fits all" solution or one target architecture that would work for all situations. 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 effort that is meant to address this IPv4 service continuity issue focuses mainly on stateful mechanisms that assume the sharing of any global IPv4 address that is left between several customers, based upon the deployment of 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. This document provides elaboration on such need.

Particularly, this document describes the motivations for stateless solutions within the context of an IPv6-enabled network as described in [RFC6180]. The following table shows the targeted space:

	Crossing IPv4 networks	IPv6-enabled networks
Stateful solution	RFC5571 (L2TP)	DS-Lite
Stateless solution	RFC5969 (6rd)	*Target* *space *

It is explicitly acknowledged by the authors of this document that both stateful and stateless solutions are required to meet Service Providers needs and constraints.

More discussions about stateless vs. stateful can be found at [RFC6144].

2. Terminology

This document makes use of the following terms:

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

Stateless 4/6 solution (or stateless solution in short): denotes a solution which does not require any user-session state (see Section 2.3 of [RFC1958]) to be maintained by any IP address sharing function in the Service Provider's network. This category of solutions assumes a dependency between an IPv6 prefix and IPv4 address. In an IPv4 address sharing context, dedicated functions are required to be 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?

This section discusses motivations for preferring a deployment of stateless 4/6 solutions. The technical and operational benefits of the stateless solutions are possible because no per-user state [RFC1958] is maintained in the Service Providers networks.

3.1. Network Architecture Simplification

The activation of this 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 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 customer number, traffic trends and the bandwidth usage need be taken into account for dimensioning purposes.

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., ASBR routers 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. In particular, stateless solutions optimizes CPE-to-CPE communication in that packets don't go through the interconnection function since the address and port mapping has been realized based on a well defined mapping schema that is known to all involved devices.

3.1.3. Logging - No Need for Dynamic Binding Notifications

Network abuse reporting requires traceability [I-D.ietf-intarea-shared-addressing-issues]. 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 CAPEX considerations). This requirement is easily met with stateless solutions.

3.1.4. No Additional Protocol for Port Control is Required

The deployment of stateless solution does not require the deployment of new dynamic signaling protocols to 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 mapping in the CPE.

3.1.5. Bandwidth Saving

In same particular network scenarios (e.g., wireless network), spectrum is very valuable and scarce resource. Service providers usually wish to eliminate unnecessary overhead to save bandwidth consumption in such environment. Service providers need to consider optimizing the form of packet processing when encapsulation is used. Since existing header compression techniques are stateful, it is expected that stateless solution minimize overhead introduced by the solution.

3.2. Operational Tasks and Network Maintenance Efficiency

3.2.1. Preserve Current Practices

Service Providers require as much as possible to preserve the same operations as for current IP networking environments.

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. In particular:

- o anycast-based schemes can be used for load-balancing and redundancy purposes.
- 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 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, constrain 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 having a sourcing policy to avoid mono-vendor deployments and to operate highly-available networks composed on multi-vendors equipment.

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 times 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 [I-D.ietf-intarea-shared-addressing-issues]; replacing implicit identification with explicit authentication will be seen as a non acceptable service regression by the end users (less Quality of Experience (QoE)).

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.boucadair-intarea-nat-reveal-analysis] are not required for the delivery of these internal services if a stateless solution is deployed.

3.3.2. No Organizational Impact

Stateless solutions rely on IP-related techniques to share and to deliver IPv4 packets over an IPv6 network. In particular, IPv4 packets are delivered without any modification to their destination CPE. As such there is 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: Since the payload of IPv4 packets is not altered in the path, services can evolve without requiring any specific function in the Service Provider's network;

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 OPEX considerations).

From a Service Provider perspective, stateless solutions are more attractive because they do less impact the current network operations and maintenance model that is widely based on stateless approaches. 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. 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.

5. IANA Considerations

No action is required from IANA.

6. Security Considerations

Except for the less efficient port randomization of and routing loops [I-D.ietf-v6ops-tunnel-loops], 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.

7. Contributors

The following individuals have contributed to this document:

Christian Jacquenet
France Telecom

Email: christian.jacquenet@orange-ftgroup.com

Pierre Levis
France Telecom

Email: pierre.levis@orange-ftgroup.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
53A,Xibianmennei Ave.
Beijing 100053
P.R.China

Phone: +86-13910750201
Email: denghui02@gmail.com

8. 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			

9. 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>>.

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

Boucadair, M., Touch, J., and P. Levis, "Analysis of Solution Candidates to Reveal the Origin IP Address in Shared Address Deployments", draft-boucadair-intarea-nat-reveal-analysis-01 (work in progress), March 2011.

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

Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for IP address sharing schemes", draft-ietf-behave-lsn-requirements-01 (work in progress), March 2011.

[I-D.ietf-intarea-shared-addressing-issues]

Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", draft-ietf-intarea-shared-addressing-issues-05 (work in progress), March 2011.

[I-D.ietf-v6ops-tunnel-loops]

Nakibly, G. and F. Templin, "Routing Loop Attack using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", draft-ietf-v6ops-tunnel-loops-07 (work in progress), May 2011.

[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), March 2011.

- [RFC1958] Carpenter, B., "Architectural Principles of the Internet", RFC 1958, June 1996.
- [RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.
- [RFC6180] Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, May 2011.
- [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-ftgroup.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

