Softwire WG M. Boucadair
Internet-Draft France Telecom
Intended status: Standards Track I. Farrer
Expires: June 2, 2013 Deutsche Telekom
S. Krishnan
Ericsson
November 29, 2012

Unified Softwire CPE
draft-bfmk-softwire-unified-cpe-00

Abstract

Transporting IPv4 packets over IPv6 is a common solution to the problem of IPv4 service continuity over IPv6-only provider networks. A number of differing functional approaches have been developed for this, each having their own specific characteristics. As these approaches share a similar functional architecture and use the same data plane mechanisms, this memo describes a specification whereby a single CPE can interwork with all of the standardized and proposed approaches to providing encapsulated IPv4 in IPv6 services.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

IPv4 service continuity is one of the major technical challenges which must be considered during IPv6 migration. Over the past few years, a number of different approaches have been developed to assist with this problem. These approaches, or modes, exist in order to meet the particular deployment, scaling, addressing and other requirements of different service provider's networks. Section 3 describes these approaches in more detail.

A common feature shared between all of the differing modes is the integration of softwire tunnel end-point functionality into the CPE router. Due to this inherent data plane similarity, a single CPE may be capable of supporting several different approaches. Users may also wish to configure a specific mode of operation.

A service provider's network may also have more than one mode enabled. Reasons for this include supporting diverse CPE clients, simplifying migration between modes or where service requirements define specific supporting softwire architectures.

In order for softwire based services to be successfully established, it is essential that the customer end-node, the service provider end-node and provisioning systems are able to indicate their capabilities and preferred mode of operation.

This memo describes the logic required by both the CPE tunnel end-node and the service provider's provisioning infrastructure so that softwire services can be provided in mixed-mode environments.

1.1. Rationale

The following rationale has been adopted for this document:

(1) Describe clear distinctions between the different solution modes
(2) Simplify solution migration paths: Define a unified CPE behavior which allows for smooth migration between the different modes
(3) Deterministic co-existence behavior: Specify the behavior when several modes co-exist in the CPE
(4) Re-usability: Maximize the re-use of existing functional blocks including Tunnel Endpoint, port restricted NAPT44, Forwarding behavior, etc.
(5) Solution agnostic: Adopt neutral terminology and avoid (as far as possible) overloading the document with solution-specific terms

(6) Flexibility: Allow operators to compile CPE software only for the mode(s) necessary for their chosen deployment context(s)
(7) Simplicity: Provide a model that allows operators to only implement the specific mode(s) that they require without the additional complexity of unneeded modes.

2. Requirements Language

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].

3. IPv4 Service Continuity Architectures: A 'Big Picture' Overview

The solutions which have been proposed within the Softwire WG can be categorized into three main functional approaches, as listed below:
(1) Full stateful approach (DS-Lite, [RFC6333]): Requires per-session state to be maintained in the Service Provider's network.
(2) Binding approach (e.g., Lightweight 4over6 (Lw4o6) [I-D.cui-softwire-b4-translated-ds-lite], [I-D.ietf-softwire-public-4over6] or MAP 1:1 [I-D.ietf-softwire-map]): Requires a single per-subscriber state (or a few) to be maintained in the Service Provider's network.
(3) Full stateless approach (MAP, [I-D.ietf-softwire-map]): Does not require per-session or per-subscriber state to be maintained in the Service Provider's network.

All these approaches share a similar architecture, using a tunnel end-node located in a CPE and a tunnel concentrator end-node located in the service provider's network. All use IPv6 as the transport protocol for the delivery of an IPv4 connectivity service using an IPv4-in-IPv6 encapsulation scheme [RFC2473].

Throughout this document, the different techniques that have been proposed to realize these different functional approaches (DS-Lite, Lw4o6, & MAP-E) are referred to as 'modes'.

3.1. Functional Elements

Table 1 lists the required functional elements for each solution mode:

Mode	Customer side	Network side
DS-Lite	B4	AFTR
Lw4o6	lwB4	lwAFTR
MAP	MAP CE	MAP BR

Table 1: Functional Elements

Table 2 describes each functional element:

Functional Element	Description
B4	An IPv4-in-IPv6 tunnel endpoint; the B4 creates a tunnel to a pre-configured remote tunnel endpoint.
AFTR	Provides both an IPv4-in-IPv6 tunnel endpoint and a NAT44 function implemented in the same node.
lwB4	A B4 which supports port-restricted IPv4 addresses. An lwB4 MAY also provide a NAT44 function.
lwAFTR	An IPv4-in-IPv6 tunnel endpoint which maintains per-subscriber address binding. Unlike the AFTR, it MUST NOT perform a NAPT44 function.
MAP CE	A B4 which supports port-restricted IPv4 addresses. It MAY be co-located with a NAT44. A MAP CE forwards IPv4-in-IPv6 packets using provisioned mapping rules to derive the remote tunnel endpoint.
MAP BR	An IPv4-in-IPv6 tunnel endpoint. A MAP BR forwards IPv4-in-IPv6 packets following pre-configured mapping rules.

+------------+--+

Table 2: Required Element Functionality

Table 3 identifies features required at the Customer's side.

Functional Element	IPv4-in-IPv6 tunnel endpoint	Port-restricted IPv4	Port-restricted NAT44
B4	Yes	N/A	No
lwB4	Yes	Yes	Optional

MAP-E CE	Yes	Yes	Optional

Table 3: Supported Features

3.2. Required Provisoning Information

Table 4 identifies the provisioning information required for each flavor.

Mode	Provisioning Information
DS-Lite	Remote IPv4-in-IPv6 Tunnel Endpoint
Lw4o6	Remote IPv4-in-IPv6 Tunnel Endpoint
	IPv4 Address
	Port Set
MAP-E	Mapping Rules
	MAP Domain Parameters

Table 4: Provisioning Information

Note: MAP Mapping Rules are translated into the following configuration parameters: Set of Remote IPv4-in-IPv6 Tunnel Endpoints, IPv4 Address and Port Set.

4. Unified Softwire CPE Behaviour

This section specifies a unified CPE behavior capable of supporting the three modes

4.1. Full IPv4 Address Assignment

All the aforementioned modes MUST be designed to allow either a full or a shared IPv4 address to be assigned to a customer end-node.

DS-Lite and MAP-E fulfill this requirement. With minor changes, the [I-D.cui-softwire-b4-translated-ds-lite] specification can be updated to assign full IPv4 addresses.

4.2. Customer Side NAT

A NAT function within the customer end-node is not required for DS-Lite, while it is optional for both MAP-E and Lw4o6.

When enabled in MAP-E and Lw4o6, the NAT MUST be able to restrict its external translated source ports to within the set of ports provisioned to the Initiator (e.g., Host, CPE).

4.3. Generic CPE Bootstrapping Logic

The generic provisioning logic is designed to meet the following requirements:

- When several service continuity modes are supported by the same CPE, it MUST be possible to configure a single mode for use.
- For a given network attachment, only one mode MUST be activated.
- The CPE MAY be configured by a user or via remote device management means (e.g., DHCP, TR-069).
- A network which supports one or several modes MUST return valid configuration data allowing requesting devices to unambiguously select a single mode to use for attachment.

This section sketches a generic algorithm to be followed by a CPE supporting one or all the modes listed above. Based on the retrieved information, the CPE will determine which mode to activate.

(1) If a given mode is enabled (DS-Lite, Lw4o6 or MAP-E), the CPE MUST be configured with the required provisioning information listed in Table 4. If all of the required information is not available locally, the CPE MUST use available provisioning means (e.g., DHCP) to retrieve the missing configuration data.

(2) If the CPE supports several modes, but no mode is explicitly enabled, the CPE MUST use available provisioning means (e.g., DHCP) to retrieve available configuration parameters and use the availability of individual parameters to ascertain which functional mode to configure:

  (2.1) If only a Remote IPv4-in-IPv6 Tunnel Endpoint is received, the CPE MUST proceed as follows:

    (2.1.1) IPv4-in-IPv6 tunnel endpoint initialization is defined in [RFC6333].

    (2.1.2) Outbound IPv4 packets are forwarded to the next hop as specified in Section 4.5.

  (2.2) If a Remote IPv4-in-IPv6 Tunnel Endpoint, an IPv4 Address and optionally a Port Set are received, the CPE MUST behave as follows:

    (2.2.1) IPv4-in-IPv6 tunnel endpoint initialization is similar to B4 [RFC6333].

    (2.2.2) When NAPT44 is required (e.g., because the CPE is a router), a NAPT44 module is enabled.

(2.2.3) The tunnel endpoint is assigned with a native IPv6 address. No particular considerations are required to be taken into account to generate the Interface Identifier.
(2.2.4) When a port set is provisioned, the external source ports MUST be restricted to the provisioned set of ports.
(2.2.5) Outbound (NATed) IPv4 packets are forwarded to the next hop as specified in Section 4.5.

(2.3) If Mapping Rule(s) are received, the CPE MUST behave as follows:
(2.3.1) IPv4-in-IPv6 tunnel endpoint initialization is similar to a B4 [RFC6333].
(2.3.2) The tunnel endpoint is assigned with an IPv6 address which includes an IPv4 address. The MAP Interface Identifier is based on the format specified in Section 2.2 of [RFC6052].
(2.3.3) When NAPT44 is required (e.g., because the CPE is a router), a NAPT44 module is enabled.
(2.3.4) When a port set is provisioned, the external source port MUST be restricted to the provisioned set of ports.
(2.3.5) Outbound (NATed) IPv4 packets are forwarded to the next hop as specified in Section 4.5.

4.4. Customer Side DHCP Based Provisioning

[DISCUSSION NOTE: As it is proposed that OPTION_MAP would be used for all new softwire provisioning, should we rename OPTION_MAP to OPTION_SW (incl. the associated sub-options)?]

DHCP-based configuration SHOULD be implemented by the customer end-node using the following two DHCP options:

OPTION_AFTR_NAME [RFC6334] Provides the FQDN for the remote IPv4-in-IPv6 tunnel end-point.

OPTION_MAP [I-D.ietf-softwire-map-dhcp] Provides IPv4-related configuration for the binding mode, mapping rules for the stateless mode, including MAP parameters (e.g., offset, domain prefix, etc). OPTION_MAP_BIND is a sub-option used to convey an IPv4 address (for example, encoded as an IPv4-mapped IPv6 address [RFC4291]). This address is used when binding mode is enabled. The receipt of OPTION_MAP_BIND is an implicit indication to the customer side device to operate in binding, rather than stateless mode.

The customer end-node uses the DHCP Option Request Option (ORO) to request either one or both of these options depending on which modes it is capable of and configured to support.

The DHCP options sent in the response allow the service provider to inform the customer end-node which operating mode to enable.

The following table shows the different DHCP options (and sub-options) that the service provider can supply in a response.

DHCP Option	Stateful Mode	Binding Mode	Stateless Mode
OPTION_AFTR_NAME	Yes	Yes	Optional
OPTION_MAP	No	Yes	No
OPTION_MAP_BIND			
OPTION_MAP	No	No	Yes
OPTION_MAP_RULE			
OPTION_MAP_PORTPARAMS	No	Optional	Optional

Table 5: DHCP Option Provisioning Matrix

The customer side device MUST interpret the received DHCP configuration parameters according to the logic defined in Section 4.3:

- o If only OPTION_AFTR_NAME is received, then the device MUST operate in stateful mode
- o If both OPTION_AFTR_NAME and OPTION_MAP_BIND are received then the device MUST operate in binding mode
- o If one or more OPTION_MAP_RULE options are received, then the customer side device MUST operate in stateless mode
- o If both OPTION_AFTR_NAME and OPTION_MAP_RULE(s) are received, then the customer side device MUST operate as a MAP CE. OPTION_AFTR_NAME provides the FQDN of the MAP BR.
- o If OPTION_MAP_PORTPARAMS is received as a sub-option to either

OPTION_MAP_BIND or OPTION_MAP_RULE, then NAPT44 MUST be configured using the supplied port-set for external translated source ports.

From the service providers side, the following rule MUST be followed:

- o The DHCP server MUST NOT send both OPTION_MAP_BIND and OPTION_MAP_RULE in a single OPTION_MAP response.

4.5. Forwarding Action by the Customer End-Node

For all modes, the longest prefix match algorithm MUST be enforced to forward outbound IPv4 packets.

Concretely, this algorithm will:
o always return the address of the AFTR for the DS-Lite mode.
o always return the address of the lwAFTR for the binding mode.
o return the next hop according to the pre-configured mapping rules for the stateless mode (i.e., MAP-E).

5. Security Considerations

Security considerations discussed in Section 7 of [I-D.ietf-softwire-stateless-4v6-motivation] and Section 11 of [RFC6333]should be taken into account.

6. IANA Considerations

This document does not require any action from IANA.

7. References

7.1. Normative References

[I-D.cui-softwire-b4-translated-ds-lite]
Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture", draft-cui-softwire-b4-translated-ds-lite-09 (work in progress), October 2012.

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., and T. Murakami, "Mapping of Address and Port with Encapsulation (MAP)", draft-ietf-softwire-map-02 (work in progress), September 2012.

[I-D.ietf-softwire-map-dhcp]
Mrugalski, T., Troan, O., Bao, C., Dec, W., and L. Yeh, "DHCPv6 Options for Mapping of Address and Port", draft-ietf-softwire-map-dhcp-01 (work in progress), August 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

7.2. Informative References

[I-D.ietf-softwire-public-4over6]
Cui, Y., Wu, J., Wu, P., Vautrin, O., and Y. Lee, "Public IPv4 over IPv6 Access Network", draft-ietf-softwire-public-4over6-04 (work in progress), October 2012.

[I-D.ietf-softwire-stateless-4v6-motivation]
Boucadair, M., Matsushima, S., Lee, Y., Bonness, O., Borges, I., and G. Chen, "Motivations for Carrier-side Stateless IPv4 over IPv6 Migration Solutions", draft-ietf-softwire-stateless-4v6-motivation-05 (work in progress), November 2012.

[RFC6334] Hankins, D. and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite", RFC 6334, August 2011.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes
France

Email: mohamed.boucadair@orange.com

Ian Farrer
Deutsche Telekom
Germany

Email: ian.farrer@telekom.de

Suresh Krishnan
Ericsson

Email: suresh.krishnan@ericsson.com