Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 7 November 2026

T. Lemon
Apple Inc.
J. Hui
Google LLC
E. Dijk
IoTconsultancy.nl

6 May 2026

Automatically Connecting Stub Networks to Unmanaged Infrastructure
draft-ietf-snac-simple-10

Abstract

This document describes a set of practices for connecting stub networks to adjacent infrastructure networks. This is applicable in cases such as constrained (Internet of Things) networks where there is a need to provide functional parity of service discovery and reachability between devices on the stub network and devices on an adjacent infrastructure link (for example, a home network).

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 https://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 7 November 2026.

Copyright Notice

Table of Contents

1. Introduction

This document describes a set of practices for automatically connecting IPv6 stub networks to adjacent infrastructure networks. The connection is enabled through a Stub Network Auto-Configuring router, or SNAC router. There are several use cases for stub networks. Motivating factors include:

* Incompatible speed: for example, an IEEE 802.15.4 network could not be easily bridged to a Wi-Fi network because the data rates are so dissimilar. So either it must be bridged in a very complicated and careful way to avoid overwhelming the 802.15.4 network with irrelevant traffic, or the 802.15.4 network needs to be a separate subnet.

* Incompatible media: for example, a constrained 802.15.4 network connected as a stub network to a Wi-Fi or Ethernet infrastructure network. In this situation bridging between the two media is not possible because the layer two framing and addressing is incompatible.

* Inconsistent availability of individual routers: In the case of an 802.15.4 network, it is quite possible that the devices used to link the infrastructure network to the stub network will not be conceived of by the end user as routers. Consequently, one cannot assume that these devices will be on all the time. A solution for this use case will require some sort of commissioning process for stub routers, and can't assume that any particular stub router will always be available; rather, any stub router that is available must be able to adapt to current network conditions to provide reachability.

* Incompatible mechanisms: the medium of the stub network may not, for example, use IPv6 Neighbor Discovery to populate a neighbor cache. If the infrastructure network (as is typical) does use Neighbor Discovery, then bridging the two networks together would require some way of translating between Neighbor Discovery and

whatever mechanism is used on the stub network, and hence complicates rather than simplifies the problem of connecting the two networks.

* Incompatible framing: if the stub network is a 6LoWPAN [RFC4944] network, packets on the stub network are expected to use 6LoWPAN header compression [RFC6282]. Making this work through a bridge would be very difficult.

* Convenience: end users often connect devices to each other in order to extend networks.

* Transitory connectivity: a mobile device acting as a stub router for a set of co-located devices could connect to an infrastructure network and gain access to services for itself and for the co-located devices. Such a stub network is unlikely to have more than one stub router.

What makes stub networks a distinct type of network is simply that a stub network never provides transit between networks to which it is connected. The term "stub" refers to the way the network is seen by the link to which it is connected: there is reachability through a stub router to devices on the stub network from the adjacent infrastructure link, but there is no reachability through the stub network to any link beyond that one.

Eliminating transit routing is not intended to be seen as a virtue in itself, but rather as a simplifying assumption that makes it possible to solve a subset of the general problem of automating multi-link networks. Stub networks may be globally reachable, or may be only locally reachable. A host on a locally reachable stub network can only interoperate with hosts on the network link(s) to which it is connected. A host on a globally reachable stub network should be able to interoperate with hosts on other network links in the same infrastructure as well as hosts on the global Internet.

It may be noted that just as one can plug several CE Router devices together in series to form multi-layer NATs, there is nothing preventing the owner of a stub router from attaching it to a stub network as if that network were its infrastructure network. In the case of an IoT wireless network, there may be no way to do this, nor would it be desirable, but a stub router that uses Ethernet on both the infrastructure and stub network sides could be connected this way. Nothing in this document is intended to prevent this from being done, but neither does this document attempt to solve the problems that this could create.

The goal of this document is to describe the minimal set of changes or behaviors required to use existing IETF specifications to support the stub network use case. The result is intended to be deployable on existing infrastructure networks without requiring changes to those networks.

1.1. Interoperability Goals

The specific goal is for hosts on the stub network to be able to interoperate with hosts on the adjacent infrastructure link. What is meant by "interoperate" is that a host on a stub network:

* is discoverable by hosts attached to the adjacent infrastructure link
* is able to discover hosts attached to the adjacent infrastructure link
* is able to discover hosts on the Internet
* is able to acquire an IP address that can be used to communicate with hosts attached to the adjacent infrastructure link
* has reachability to the hosts attached to the adjacent infrastructure link
* is reachable by hosts on the adjacent infrastructure link
* is able to reach hosts on the Internet

Discoverability here means "discoverable using DNS, or DNS Service Discovery". DNS Service Discovery includes multicast DNS [RFC6762]. As an example, when one host connected to a specific Wi-Fi network wishes to discover services on hosts connected to that same Wi-Fi network, it can do so using multicast DNS. Similarly, when a host on some other network wishes to discover the same service, it must use DNS-based Service Discovery [RFC6763]. In both cases, "discoverable using DNS" means that the host has one or more entries in the DNS that serve to make it discoverable.

Discoverability is lumped in with reachability and addressability, both of which are essentially Layer 3 issues. The reason for this is that it does no good to automatically set up connectivity between stub network hosts and infrastructure hosts if the infrastructure hosts have no means to learn about the availability of services provided by stub network hosts. For stub network hosts that only consume Internet services this will not be an issue, but for stub networks that provide services, such as IoT devices on stub networks with incompatible media, discoverability is necessary in order for stub network connectivity to be useful.

Ability to acquire an IP address that can be used to communicate means that the IP address a host on the stub network acquires can be used to communicate with it by hosts not on the stub network.

Reachability to hosts on the adjacent infrastructure link means that when a host (A) on the stub network has a datagram destined for the IP address of a host (B) on the adjacent infrastructure link, host (A) knows of a next-hop router to which it can send the datagram, so that it will ultimately reach host (B) on the infrastructure network.

Reachability from hosts on the adjacent infrastructure link means that when host (A) on the adjacent infrastructure link has a datagram destined for the IP address of a host (B) on the stub network, a next-hop router is known by host (A) such that, when the datagram is sent to that router, it will ultimately reach host (B) on the stub network.

To achieve the reachability goal described above, this document assumes hosts attempting to reach destinations on the stub network maintain a routing table -- Type C hosts as defined in Section 3.1 of [RFC4191]. Type A and Type B hosts are out-of-scope for this document.

1.2. Usability Goals

In addition to the interoperability goals described above, the additional goal for stub networks is that these be able to be connected automatically, with no user intervention. The experience of connecting a stub network to an infrastructure network should be as straightforward as connecting a new host to the same infrastructure network.

SNAC routers can be attached to any network. However, there are network configurations where a SNAC router will not work. An analysis of networks where SNAC routers could be attached is provided in Appendix A.

1.3. Sample SNAC Routers Deployment in a Home Network

A stub network is attached via one or more SNAC routers to an infrastructure network. An infrastructure router in the scope of this specification is an IPv6 (aware) router that provides various services in the infrastructure network. It can be a CE router, home gateway or Wi-Fi router. A SNAC router will connect as any other host in the infrastructure network, while additionally providing addressability, discoverability and reachability functions for hosts in the stub network. See Section 8 for an overview of the specific services that a SNAC router implements to provide addressability, discoverability and reachability.

This document describes mechanisms for connecting IPv6 hosts in stub networks to the infrastructure network using SNAC routers as shown in Figure 1. Although the use case depicted there is specific to home networks, the mechanisms apply for any type of infrastructure network and stub network attachment scenarios.

A SNAC router looks for a suitable IPv6 on-link prefix on the adjacent infrastructure link (AIL) to which it is connected. This prefix may be already provided by the infrastructure router, or when no IPv6 infrastructure service is present, by another SNAC router connected to the same AIL. If no suitable IPv6 on-link prefix is advertised on the AIL, the SNAC router will provide one itself using its own Router Advertisement messages.

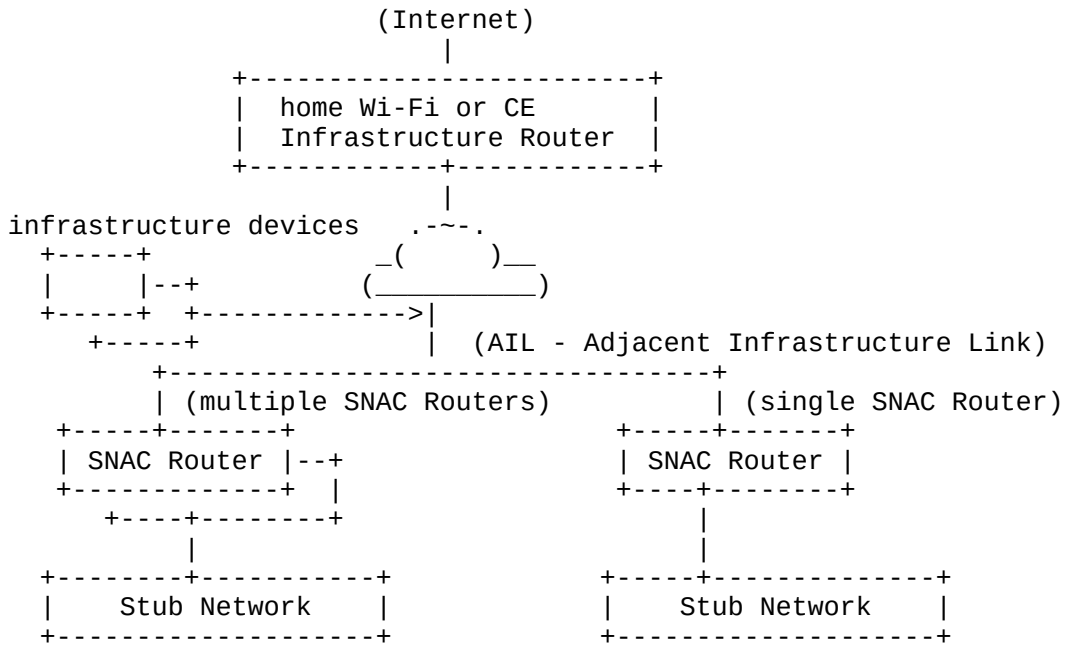

Figure 1: SNAC Router connecting Stub Networks to Infrastructure

2. Glossary

This section contains a glossary of terms used in this document. See Section 4 for document conventions and remaining terms and definitions.

Node: A device that implements IPv6.

Router: A node that forwards IPv6 packets not explicitly addressed to itself. (See Note in Section 2 of [RFC8200].)

Host: Any node that is not a router. (See Note in Section 2 of [RFC8200].)

Addressability: The ability to associate each node on a link with its own IPv6 address.

Reachability: Given an IPv6 destination address that is not on-link for any link to which a node is attached, the information required that allows the node to send packets to a router that can forward those packets towards a link where the destination address is on-link.

Adjacent Infrastructure Link (AIL): any link to which a stub router is directly attached, that is part of an infrastructure network and is not the stub network.

Customer Edge (CE) Router: CE Router is defined in [RFC7084]. A CE router is an infrastructure router that is intended to connect a single uplink network to a Local-Area Network. A CE router may be provided by an ISP and only capable of connecting directly to the ISP's means of service delivery, e.g. Cable or DSL, or it may have an Ethernet port on the WAN side and one or more Ethernet ports, plus Wi-Fi, on the LAN side.

Infrastructure network: the network infrastructure to which a stub router connects. This network can be a single link, or a network of links. The network is formed by one or more infrastructure routers. In a home network, this is typically a CE router, which may also provide some services, such as a DNS resolver, a DHCPv4 server, and a DHCPv6 prefix delegation server, for example.

Infrastructure router: An IP router that is part of an infrastructure network. For example, a CE router.

Off-Stub-Network-Routable (OSNR) Prefix: an IPv6 prefix advertised on the stub network that can be used for communication with hosts not on the stub network.

Stub Network: A network link that is connected by one or more stub routers to an AIL in an infrastructure network, but is not used for transit between that link and any other link. Section 2.1 of [RFC2328] describes the distinction between stub networks and transit networks from a topological perspective: a stub network is simply any network that does not provide transit within a routing fabric. There is reachability through a stub network router to hosts on the stub network, but there is no reachability through the stub network to any link beyond the stub network link.

Stub Router: A router that provides connectivity between a stub network and an infrastructure network. A stub router may also provide connectivity between other networks: the term "stub router" refers specifically to its role in providing connectivity to a stub network. For example, a CE Router may provide connectivity between a provider network (WAN) and a network (LAN), while at the same time providing connectivity between the LAN and a stub network. What distinguishes the LAN from the stub network in this case is that the LAN is potentially a candidate to act as a transit network to reach other routers, whereas the stub network is not.

SNAC Router: A Stub Network Auto-Configuring (SNAC) Router. This is a stub router that implements the autoconfiguration methods defined by this specification. By definition, a CE router can't be a SNAC router, because it is an infrastructure router, and therefore has operational control over its stub networks.

ULA Site Prefix: A Unique Local Address /48 prefix [RFC4193] randomly generated by each SNAC router for use in allocating ULA link prefixes to the stub network and the adjacent infrastructure link.

ULA Link Prefix: A Unique Local Address /64 prefix allocated from the ULA site prefix. SNAC routers can use ULA link prefixes to provide addressability on the stub network and/or adjacent infrastructure link as needed. If a SNAC router is doing NAT64 [RFC6146], the NAT64 prefix is also a ULA link prefix. A total of 65,536 ULA link prefixes can be allocated from the ULA site prefix.

3. Constants

This section describes the meaning of and gives default values for various constants used in this document.

STALE_RA_TIME (default: 10 minutes): The amount of time that can pass after the last time a Router Advertisement (RA) message from a particular router has been received before it is assumed the router is no longer present. This is a stopgap in case the router is reachable but has silently stopped advertising a prefix; this situation is unlikely, but if it does happen, new devices joining the infrastructure network will not be able to reach devices on the stub network until the SNAC router decides that the router that advertised the suitable prefix is stale.

STUB_PROVIDED_PREFIX_LIFETIME (default: 30 minutes): The valid and preferred lifetime the SNAC router will advertise for a prefix on the AIL. This should be long enough that a host is actually willing to use it, and obviously should also be long enough that a missed RA will not cause the host to stop using it. The values suggested here allow ten RAs to be missed before the host will stop using the prefix.

MinRtrAdvInterval (default: 154 seconds): The minimum interval for periodic unsolicited RA message sending (as defined in [RFC4861]) for a SNAC router. This determines together with MaxRtrAdvInterval how often the SNAC router will transmit these multicast RA messages. This should be frequent enough that a missed Router Solicitation (RS) message (e.g. due to congestion on

a Wi-Fi link) will not result in an extremely long outage (assuming the congestion passes before the RA is sent, of course). The default values defined here lead to an RA multicast every 3 minutes, on average.

MaxRtrAdvInterval (default: 206 seconds): The maximum interval for periodic unsolicited RA message sending (as defined in [RFC4861]) for a SNAC router.

MIN_PD_PREFIX_LIFETIME (default: 30 minutes): The minimum preferred lifetime that a prefix, delegated with DHCPv6-PD, must have in order to be suitable as a OSNR prefix for the stub network. The minimum lifetime is chosen to be long enough that a reboot of the DHCP server or the SNAC router will not prevent the successful renewal of the prefix.

MAX_SUITABLE_REACHABLE_TIME (default: 60 seconds): The maximum ReachableTime value that a router can have in the neighbor cache before any suitable prefixes it has advertised are no longer considered suitable.

STUB_NETWORK_ROUTE_LIFETIME (default: 30 minutes): The Route Lifetime that will be specified in Route Information Options (RIOs) sent by the SNAC router to advertise the route to its stub network on the AIL. Also, the maximum Route Lifetime that will be specified in Route Information Options sent by the SNAC router to its stub network to advertise the route to the AIL.

MIN_SUITABLE_PREFIX_PREFERRED_LIFETIME (default: 30 minutes): The minimum preferred lifetime required for an AIL prefix to be considered suitable for use by SNAC routers. This value ensures that prefixes have sufficient lifetime to be reliably used for address autoconfiguration and communication establishment.

4. Conventions and Terminology Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The terms "resolver" and "stub resolver" used in this document are defined in [RFC9499]. "DNS resolver" is used as a synonym for "resolver" to clearly point out the DNS context of this term.

The term "advertising interface" is used as defined in Section 6.2.2 of [RFC4861].

5. Maintenance of addressability on AIL and stub network links

This document assumes that the AIL supports Neighbor Discovery [RFC4861], and specifically that routers and on-link prefixes can be advertised using Router Advertisement messages and discovered using Router Solicitation messages. The stub network link may also support this, or may use some different mechanism. This section specifies how advertisement of the on-link prefix for such links is managed.

When a SNAC router sends a Router Advertisement (RA) message as specified in this document, it MUST NOT use multiple RA messages with each containing a subset of the options. Such splitting behavior is specified in Section 6.2.3 of [RFC4861]. Instead, all options are always included in a single RA message. Multiple RA messages with different information contents are only sent to indicate that previously sent information changed.

As part of standard IPv6 router behavior on the AIL interface, the SNAC router MUST join the All-Routers link-local multicast address (FF02::2) to receive Router Solicitation messages and other host-to-router and router-to-router communications, and MUST join the All-Nodes link-local multicast address (FF02::1) to receive Neighbor Solicitation messages and other host-to-host communications as described in [RFC4861]. If neighbor discovery, including Router Advertisements, is being used on the stub network, the SNAC router MUST similarly join these two multicast groups on the stub network interface as well.

A network topology of a single stub network connected via SNAC routers to more than one AIL is explicitly out of scope of this document; such a topology will likely have a negative effect on the reachability and discoverability of hosts. If a SNAC router is able to determine that an AIL (other than its own) is already in use for its stub network, for example provided by one or more other SNAC routers or by other router types, it is advised that the SNAC router takes appropriate actions such as warning the user or ceasing to operate as a SNAC router until the situation is resolved. How a stub router might detect this situation is however out of scope for this document.

5.1. Maintenance across SNAC router restarts

SNAC routers may restart from time to time; when a restart occurs, the SNAC router may have been advertising state to the network which, following the restart, is no longer required.

For example, suppose there are two SNAC routers connected to the same adjacent infrastructure link. When the first SNAC router is restarted, the second takes over providing an on-link prefix. Now the first router rejoins the link. It sees that the second SNAC router's prefix is advertised on the adjacent infrastructure link, and therefore does not advertise its own.

This behavior can cause problems because the first SNAC router no longer sees the on-link prefix it had been advertising on infrastructure as on-link. Consequently, if it receives a packet on the stub network with a destination address matching this prefix, it will forward that packet directly to a default router, if one is present; otherwise, it will have no route to the destination, and will drop the packet.

This amounts to a flash renumbering event. There is no easy way to prevent this from happening: routes and prefixes advertised in Router Advertisement messages have lifetimes, and hosts may continue to use the included prefixes until they expire. Applications that are not able to detect the loss of a route or that do not quickly notice that a host is no longer reachable on a particular address will exhibit poor performance when this happens. For example, if the stub network is a network that supports IoT devices, the user may experience temporary inability to control such devices, and automations may fail.

When possible, it is best if all SNAC routers serving a particular stub network use the same /64 on-link prefix for the AIL. For example, Thread [Thread] SNAC routers use bits from the Thread Extended PAN ID to generate the ULA prefix's Global ID and Subnet ID. The Global ID generation conforms to [RFC4193] because the Extended PAN ID is generated randomly using the same mechanism that is specified in RFC 4193 for the ULA prefix bits.

Because the Extended PAN ID is a stable value that identifies the Thread network, it can be safely used to number the adjacent infrastructure link when no other suitable on-link prefix is available, and since it can be maintained by all Thread SNAC routers, there are no problems due to a change of the AIL on-link prefix. Of course, when SNAC routers supporting more than one such stub network are present, the problem still exists in principle, but as long as all SNAC routers supporting a single stub network do not restart at the same time, the AIL on-link prefix can be expected to remain stable.

Similarly, it can be the case that while a SNAC router is advertising the sole OSNR prefix on the stub network, it is rebooted or updated. In this case, if other SNAC routers are present, they can continue to

advertise routes to that prefix on the stub network. If possible, the original OSNR prefix SHOULD be preserved until the SNAC router that advertised it returns. However, if a host on the stub network multicasts a Router Solicitation message to the link and the SNAC router advertising the OSNR prefix is still not present, or if the OSNR prefix is in danger of expiring, another SNAC router needs to take over and advertise its OSNR prefix. In this situation, SNAC routers that remember the old OSNR prefix continue advertising a route to it on the AIL until the OSNR prefix expires.

6. Support for adjacent infrastructure links

Support for AILs on networks where Neighbor Discovery is not supported is out of scope for this document. SNAC routers do not provide routing between AILs when connected to more than one such link.

6.1. Managing addressability on an adjacent infrastructure link

In order to provide IPv6 routing to the stub network, IPv6 addressing must be available on the AIL a SNAC router is attached to. Ideally such addressing is already present on the AIL, and need not be provided. However, if it is not present, the SNAC router must provide it.

6.1.1. Suitable On-Link Prefixes

SNAC routers must evaluate prefixes that are advertised on-link as to their suitability for use in communicating with devices on the stub network. If no suitable prefix is found, a SNAC router MUST advertise one.

An on-link prefix is considered suitable if it is advertised on the link in a Prefix Information option ([RFC4861], Section 4.6.2) with the following Prefix Information option header values:

* Prefix Length is 64, suitable for IPv6 Stateless Address Autoconfiguration (SLAAC), consistent with current implementations of 64-bit interface identifiers in Section 2.5.1 of [RFC4291],

* ’L’ flag bit is set and

* either the ’A’ flag bit or the ’P’ flag bit [RFC9762] is set, and

* Preferred Lifetime of MIN_SUITABLE_PREFIX_PREFERRED_LIFETIME or higher.

A prefix is not considered a suitable on-link prefix if the ’L’ flag bit is not set, or if neither the ’A’ flag bit nor the ’P’ flag bit are set. When the ’A’ flag bit is not set, this indicates that individual node addresses cannot be configured with SLAAC. In this case, typically addresses are managed using DHCPv6, or (in rare cases) another method. If the ’P’ flag bit is set, then hosts that wish to allocate their own addresses can do so by acquiring a prefix from which to allocate them using DHCPv6 prefix delegation [RFC9663]. Nodes are not required to use DHCPv6 to acquire individual addresses, so a prefix that requires the use of DHCPv6 for that purpose can’t be considered "suitable"—not all hosts can actually use it.

Note: there can be layer-two networks where Neighbor Discovery is not supported and therefore the ’L’ flag bit cannot be set, while the ’A’ flag bit could be set. The behavior of SNAC routers when connecting to such networks is out of scope for this document.

A prefix is considered to be advertised on the link if, when a Router Solicitation message ([RFC4861], Section 4.1) is sent, a Router Advertisement message is received in response which contains a Prefix Information option ([RFC4861], Section 4.6.2) for that prefix.

After an RA message containing a suitable prefix has been received, it can be assumed for some period of time thereafter that that prefix is still valid on the link. However, prefix lifetimes and router lifetimes are often quite long. In addition to knowing that a prefix has been advertised on the link in the past, and is still valid, it must therefore be ensured that at least one router that has advertised this prefix is still alive to respond to Router Solicitation messages.

6.1.2. State Machine for maintaining a suitable on-link prefix on an adjacent infrastructure link

The possible states of an interface connected to an AIL are described here, along with actions required to be taken to monitor the state. The purpose of the state machine described here is to ensure that at all times, when a new host arrives on the AIL, it is able to acquire an IPv6 address on that link.

During all of the states mentioned here except for state-unknown, the SNAC router is expected to treat the infrastructure interface as an advertising interface as described in Section 6.2.2 of [RFC4861]. There are two sets of information that need to be sent in an RA; if neither is present, then the SNAC router SHOULD NOT send an RA even if it is treating the infrastructure interface as an advertising interface.

These two sets of information are the on-link prefix, if any, that is to be advertised. Whether or not such a prefix is advertised, and what exactly is advertised regarding that prefix, is determined by the state machine. The other set of information is a set of routes to prefixes on the stub network. Whenever the SNAC router knows of a reachable (scope is not link-local and not realm-local) prefix on the stub network, it includes an RIO option in the RA on the infrastructure network indicating that that prefix is reachable through the SNAC router.

It is important to note that it is possible for an OSNR prefix to be advertised and then withdrawn on the stub network, but for it to still be valid, and for there to still be some communication occurring using that prefix. In order to avoid prematurely interrupting such communication, the SNAC router MUST maintain a list of prefixes known to be valid on the stub network, even if those prefixes have been deprecated, and MUST include RIO options for all such prefixes in the RAs that it sends on the adjacent infrastructure link.

When a SNAC router enables its AIL interface as an advertising interface and determines it needs to send unsolicited RAs per Section 6.2.4 of [RFC4861], it MUST use a random delay between 0 and MAX_INITIAL_RTR_ADVERT_INTERVAL, instead of the effectively fixed delay of MAX_INITIAL_RTR_ADVERT_INTERVAL currently specified by [RFC4861].

6.1.2.1. Status of IP addressability on adjacent infrastructure link unknown (STATE-UNKNOWN)

When the SNAC router interface first connects to the AIL, it MUST begin router discovery.

If, after router discovery has completed, no suitable on-link prefix has been found, the router moves this interface to STATE-BEGIN-ADVERTISING (Section 6.1.2.3).

If, during router discovery, a suitable on-link prefix is found, the router moves the interface to STATE-SUITABLE (Section 6.1.2.2).

In this state, the SNAC router MUST NOT treat this interface as an advertising interface as described in Section 6.2.2 of [RFC4861].

6.1.2.2. IP addressability already present on adjacent infrastructure link (STATE-SUITABLE)

When a new host appears on the AIL and sends an initial Router Solicitation message, if it does not receive a suitable on-link prefix in a Router Advertisement, it will not be able to communicate. Consequently, the SNAC router MUST monitor Router Solicitation and Router Advertisement messages on the interface in order to determine whether a prefix that has been advertised on the link is still being advertised. To accomplish this, the SNAC router uses two complementary methods: router staleness detection and neighbor unreachability detection.

6.1.2.2.1. Router staleness detection

The SNAC router MUST listen for Router Advertisement messages on the AIL to which the interface is attached, and record the time at which each Router Advertisement was received. The router MUST NOT consider any Router Advertisement that is older than STALE_RA_TIME to be suitable. When the last non-stale Router Advertisement message containing a suitable prefix on the link is marked stale, the SNAC router MUST move the interface to STATE-BEGIN-ADVERTISING.

6.1.2.2.2. Router Unreachability Detection

For each suitable prefix, the SNAC router MUST monitor the state of reachability to the router(s) that advertised it as described in ([RFC4861], Section 7.3.1) using a ReachableTime value of no more than MAX_SUITABLE_REACHABLE_TIME. The reason for this is that if no router providing the on-link prefix on the AIL is reachable, then when a new host joins the network, it will have no suitable on-link prefix to use for autoconfiguration, and thus will be unable to communicate with hosts on the stub network.

Whenever the ReachableTime for a router advertising a suitable prefix exceeds MAX_SUITABLE_REACHABLE_TIME, the SNAC router MUST send unicast Neighbor Solicitation messages as described in Section 7.2.2 of [RFC4861] until either a response is received, which resets ReachableTime to zero, or the maximum number of retransmissions has been sent.

The SNAC router MUST listen for Router Solicitation messages on the AIL. When a Router Solicitation message is received, if none of the on-link routers on the AIL are marked reachable, the SNAC router MUST move this interface to the STATE-BEGIN-ADVERTISING state (Section 6.1.2.3).

If the scheduled time for sending a periodic unsolicited multicast RA message arrives, and there are no routers advertising suitable prefixes that have a ReachableTime that is less than MAX_SUITABLE_REACHABLE_TIME, then the router MUST move this interface to the STATE-BEGIN-ADVERTISING state.

6.1.2.3. IP addressability not present on adjacent infrastructure link (STATE-BEGIN-ADVERTISING)

In this state, the SNAC router generates its own on-link prefix for the AIL. This prefix has a valid and preferred lifetime of STUB_PROVIDED_PREFIX_LIFETIME seconds. The SNAC router sends a Router Advertisement (RA) message containing this prefix in a Prefix Information option (PIO). In the PIO, the 'A' flag bit (autonomous address configuration), see Section 4.6.2 of [RFC4861], MUST be set and the 'L' flag bit (on-link) MUST also be set. Link-layer technologies that require the 'L' flag bit to be cleared are out of scope of this document.

The 'SNAC Router' flag bit ([I-D.ietf-6man-snac-router-ra-flag]) MUST be set in the RA flags field. The values of the 'M' and 'O' flag bits MUST be copied from the respective 'M' and 'O' flag bit values seen in the most recent (unicast or multicast) RA received from a non-SNAC-router. For the selection of the most recent RA, the following RAs MUST be excluded:

* An RA received from a router longer ago than the Router Lifetime period indicated in the RA header. This only applies for a non-zero Router Lifetime value.

If there is no recent RA received from a non-SNAC-router, both 'M' and 'O' flag bits MUST be cleared.

The sent Router Advertisement message MUST also include a Route Information Option (Section 2.3 of [RFC4191]) for each OSNR prefix advertised on the stub network.

After having sent the initial Router Advertisement, the SNAC router moves the interface into the STATE-ADVERTISING-SUITABLE state (Section 6.1.2.4).

6.1.2.4. IP addressability provided by the SNAC router (STATE-ADVERTISING-SUITABLE)

When entering this state, the SNAC router MUST begin treating the interface as an advertising interface as described in Section 6.2.2 of [RFC4861] if it is not already doing so.

The SNAC router sends a periodic unsolicited multicast Router Advertisement message, using the format described in Section 6.1.2.3, at a random time between MinRtrAdvInterval and MaxRtrAdvInterval.

The SNAC router may receive a Router Advertisement message containing one or more suitable on-link prefixes on the AIL. If any of these prefixes are different from the prefix the SNAC router is advertising as the on-link suitable prefix, and the 'SNAC Router' flag bit is not set in the Router Advertisement flags field, the SNAC router moves the interface to STATE-DEPRECATING (Section 6.1.2.5).

If the 'SNAC Router' flag bit is set in the RA header flags field, then one of the following must be true in order for that prefix to be considered suitable:

* The prefixes are equal. In this case, the interface remains in STATE-ADVERTISING-SUITABLE.

* The prefix the SNAC router is advertising is a ULA prefix [RFC4193], and the received prefix is a non-ULA prefix. In this case, the interface moves into the STATE-DEPRECATING (Section 6.1.2.5) state.

* Both prefixes are ULA prefixes, and the received prefix, considered as a 128-bit big-endian unsigned integer, is numerically lower, then the interface moves to STATE-DEPRECATING (Section 6.1.2.5).

* Otherwise the interface remains in STATE-ADVERTISING-SUITABLE.

6.1.2.5. SNAC router deprecating the on-link prefix it is advertising (STATE-DEPRECATING)

On entry to this state, the SNAC router has been treating the interface as an advertising interface as described in Section 6.2.2 of [RFC4861], and MUST continue to do so.

When the SNAC router has detected the availability of a suitable on-link prefix on the AIL to which the interface is attached, and that prefix is preferable to the one it is advertising, it continues to advertise its own prefix, but deprecates it:

* the preferred lifetime for its prefix should be set to zero in subsequent Router Advertisement messages.

* the valid lifetime for its prefix should be reduced with each subsequent Router Advertisement message.

* the usability of the infrastructure-provided on-link prefix should be monitored as in the STATE-SUITABLE state; if during the deprecation period, the SNAC router detects that there are no longer any suitable prefixes on the link, as described in Section 6.1.2.2.1 or in Section 6.1.2.2.2, it MUST return the interface to the STATE-BEGIN-ADVERTISING (Section 6.1.2.3) state and resume advertising its prefix with the valid and preferred lifetimes described there.

In this state, the valid lifetime (VALID) is computed based on three values: the current time when a Router Advertisement message is being generated (NOW), the time at which the new suitable on-link prefix advertisement was received (DEPRECATE_TIME), and STUB_PROVIDED_PREFIX_LIFETIME. All of these values are in seconds. VALID is computed as follows:

VALID = STUB_PROVIDED_PREFIX_LIFETIME - (NOW - DEPRECATE_TIME)

If VALID is less than MaxRtrAdvInterval seconds, the SNAC router does not include the deprecated prefix in the Router Advertisement. Note that VALID could be less than zero. Otherwise, the prefix is provided in the advertisement, but with a valid lifetime of VALID.

If no more deprecated prefix(es) are included in its Router Advertisements, the deprecation is complete and the SNAC router returns to the state STATE-SUITABLE (Section 6.1.2.2).

6.2. Managing addressability on the stub network

How addressability is managed on stub networks depends on the nature of the stub network. For some stub networks, the SNAC router can be sure that it is the only router. For example, a SNAC router that is providing a Wi-Fi network for tethering [Tethering] will advertise its own SSID and use its own joining credentials; in this case, it can assume that it is the only router for that network, and advertise a default route and on-link prefix just like any other router.

However, some stub networks are more cooperative in nature, for example IP mesh networks. On such networks, multiple SNAC routers may be present and be providing addressability and reachability.

In either case, one SNAC router connected to the stub network MUST provide a suitable on-link prefix (the OSNR prefix) for the stub network. If the stub network is a multicast-capable medium where Router Advertisement messages are used for router discovery, the same mechanism as described in Section 6.1.2 is used.

Stub networks that do not support the use of Router Advertisements for router discovery need to use some similar mechanism that is compatible with that type of network. Describing the process of establishing a common OSNR prefix on such networks is out of scope for this document. Some informative discussion on this topic is in Appendix D.

6.2.1. Generating a per-SNAC-router ULA Site Prefix

In order to be able to provide addressability either on the stub network or on the adjacent infrastructure link, a SNAC router MUST allocate its own ULA site prefix. ULA prefixes, described in Unique Local IPv6 Unicast Addresses ([RFC4193]) are randomly allocated prefixes. A SNAC router MUST allocate a single ULA site prefix for use in providing on-link prefixes to the stub network and the adjacent infrastructure link as described in Section 6.1.2.3.

Any ULA link prefixes allocated by a SNAC router SHOULD persist across reboots, and SHOULD remain stable over time. An exception to both these requirements is the following: for privacy reasons, a SNAC router that detects that its AIL changes SHOULD allocate a different ULA site prefix for the new AIL. On the latter requirement there are two possible exceptions:

1. The SNAC router remains connected to the same stub network, and the ULA site prefix value is generated based on properties of the stub network (such as configuration data - an example is the Thread Extended PAN ID detailed in Section 5.1).

2. The SNAC router is configured by the user or an operator to behave otherwise.

One implementation strategy to meet the above privacy requirement is to use the algorithm of Section 5 of [RFC7217] to generate "random but stable" bits (RID) for the ULA site prefix. This will have the property that a SNAC router will reuse its prior ULA site prefix when it is reattached again to a particular AIL where it had been attached to before.

6.2.2. Using DHCPv6 Prefix Delegation to acquire a prefix to provide addressability

If DHCPv6 prefix delegation and IPv6 service are both available on the adjacent infrastructure link, and the SNAC router has detected that it needs to provide an OSNR prefix for its stub network, then the SNAC router MUST attempt to acquire a prefix using DHCPv6 prefix delegation. Using an OSNR prefix provided by the infrastructure DHCPv6 prefix delegation service means (assuming the infrastructure

is configured correctly) that routing is possible between the stub network links and all links on the infrastructure network, and possibly to the general Internet.

By contrast, if the ULA prefix generated by the SNAC router is used, reachability is only possible between the stub network and the AIL. The OSNR prefix in this case is not known to the infrastructure network routing fabric, so even though packets might be able to be forwarded to the intended destination, there would be no return path. So when the only OSNR prefix that is available is the one generated by the SNAC router, cloud services will not be reachable via IPv6, and infrastructure-provided NAT64 will not work. Therefore, when the SNAC router is able to successfully acquire one or more prefixes using DHCPv6 PD, it MUST use an acquired prefix rather than the ULA link prefix it allocated for the stub network. Although only one acquired prefix is needed to provide the OSNR prefix for the stub network, there are reasons to acquire multiple prefixes, as detailed in the remainder of this section.

A SNAC router MUST request one or more delegated prefixes of length 64. It does so by sending an IA_PD option for each prefix, each with a different IAID, containing an IA Prefix option with a hint for length 64 as described in Section 18.2.1 of [RFC9915]. If the SNAC router obtains a prefix with length less than 64, it SHOULD generate a /64 from the obtained prefix by padding with zeros. If the SNAC router obtains a prefix with length greater than 64, the SNAC router MUST treat the prefix as unsuitable. If no suitable prefix is obtained using DHCPv6 PD, it MUST use the allocated ULA link prefix for the stub network instead.

When multiple prefixes are available for delegation (e.g., both Global Unicast Address (GUA) and Unique Local Address (ULA) prefixes), a SNAC router MUST select prefixes based on the following criteria, evaluated in order:

* Single OSNR prefix constraint: For constrained stub networks (e.g., 6LoWPAN, Thread mesh networks) that have limited support for multiple OSNR prefixes, a SNAC router MUST select only the single best prefix. Prefix type GUA MUST be preferred over ULA, then the prefix with the longest preferred and valid lifetimes is chosen for distribution.

* Multiple OSNR prefix constraint: For stub networks without a single OSNR prefix constraint, the GUA and ULA prefixes with the longest preferred and valid lifetimes are chosen for distribution. Distributing both GUA and ULA prefixes allows hosts to decide how they will communicate.

The timeout/lifetime-based selection ensures that the stub network avoids frequent renumbering events that can disrupt ongoing communications and create excessive maintenance overhead. A SNAC router SHOULD monitor delegated prefix lifetimes and re-evaluate prefix selection when lifetimes are renewed or when new prefixes become available.

A SNAC router MUST check in the server's Advertise message that the preferred lifetime a DHCPv6-PD server can offer is at least MIN_PD_PREFIX_LIFETIME prior to requesting a prefix delegation to that server. If no DHCPv6-PD server can offer this, the SNAC router MUST treat all potential DHCPv6-PD prefixes as unsuitable and use the ULA link prefix allocated for the stub network instead.

DHCPv6-PD leases obtained by a SNAC router, but not used because the prefix is not usable, MUST be released.

6.2.2.1. Lifetime of IPv6 prefixes acquired using DHCPv6 Prefix Delegation

It is possible that a SNAC router might obtain a prefix from a DHCPv6 server using prefix delegation and then something about the infrastructure network attachment might change that affects the validity of that prefix for use on the stub network. The section of [RFC9915] titled "Refreshing Configuration Information" discusses the various scenarios that can occur. The DHCPv6 prefix delegation client being used by the SNAC router is assumed to conform to this specification.

Situations that can occur include (but are not limited to):

* DHCPv6 server becomes unavailable

* SNAC router is moved to a different link

* A renumbering event results in the old prefix being replaced with a new one

The SNAC router MUST NOT use a prefix once the DHCPv6-PD client has determined that it is no longer valid. If the DHCPv6-PD client provides a new prefix, and the old prefix is still valid, the SNAC router SHOULD explicitly deprecate the old prefix at the same time that it first advertises the new prefix.

If the DHCPv6-PD client determines that the prefix it provided to use as the OSNR prefix is no longer valid, and no replacement prefix is provided by the DHCPv6 server, then the SNAC router MUST switch to the ULA link prefix that it has allocated for use on the stub

network. In the case that the DHCPv6-PD client is unable to renew its lease on the current OSNR prefix, and time between the T2 interval for the prefix assignment (Section 21.4 of [RFC9915]) and the end of the lease has been reached, then the SNAC router MUST deprecate the DHCPv6-PD-provided OSNR prefix and begin advertising the ULA link prefix.

A failure to renew the DHCPv6-PD-provided OSNR prefix could be because the SNAC router has been disconnected from one AIL and moved to a different AIL. In this situation, if the new AIL also has IPv6 service and DHCPv6-PD service, the DHCPv6 client will get a clear indication that the old prefix is no longer valid. However, it may be that no DHCPv6-PD service is available on the new link, either because it is an IPv4-only link or because it’s an IPv6-capable link that doesn’t provide DHCPv6 service. In this situation, if the SNAC router remains connected to the link and no DHCPv6 service appears, the DHCPv6-PD-provided OSNR prefix will eventually time out and be replaced. The SNAC router SHOULD NOT attempt to replace it prior to this normal timeout process, because there is no benefit to changing the OSNR prefix on the stub network in such a situation, and it’s possible that the SNAC router will return to the other link before the OSNR prefix expires.

6.3. Managing reachability on the adjacent infrastructure link

A SNAC router MUST advertise reachability to stub network OSNR prefixes on its AIL interface using Router Advertisement messages. If the SNAC router is also advertising a suitable on-link prefix for the AIL, it MUST combine the OSNR route advertisements (RIOs) and the on-link prefix advertisement (PIO) in the same Router Advertisement message, to avoid unnecessary multicast traffic.

Each stub network will have some set of prefixes that are advertised as on-link for that network. A SNAC router connected to that stub network SHOULD advertise reachability to all such prefixes on the AIL to which it is attached using Router Advertisements.

A SNAC router MUST NOT advertise itself as a default router on its AIL by setting a non-zero Router Lifetime value in the header of its Router Advertisements.

In case a new OSNR prefix is configured for its stub network (i.e. one which was not previously advertised on the AIL), a SNAC router SHOULD proactively advertise this new prefix on its AIL as defined in Section 6.2.4 of [RFC4861], fourth paragraph. The exception case is where the SNAC router detects that another router is already advertising a route to this new OSNR prefix on the AIL: in this case, the SNAC router is allowed to skip the proactive advertising.

6.4. Managing reachability on the stub network

The SNAC router SHOULD advertise itself as a default router on the stub network, if it detects that a default route is present on the AIL. In some cases it may not be desirable to advertise reachability to the Internet as a whole; for such cases the SNAC router MAY be administratively configured to not advertise itself as a default router, or it MAY use an automated policy to make such a decision.

A SNAC router MUST NOT advertise a default route lifetime on its stub network that is higher than the remaining default router lifetime on the AIL. Also, when a SNAC router detects that the default route on the AIL is not available anymore (e.g. based on a received Router Advertisement message, or detecting that the default router is no longer available), it MUST stop advertising itself as a default router on the stub network. On a stub network that supports IPv6 ND, this is done by sending its Router Advertisement messages with a zero value in the Router Lifetime field.

If the SNAC router is not advertising itself as a default router on the stub network, it MUST advertise reachability to any prefixes that are being advertised as on-link on its AIL. This is true for prefixes it is advertising, and for other prefixes being advertised on that link.

Note that in some stub network configurations, it is possible for more than one SNAC router to be connected to the stub network, and each SNAC router may be inadvertently connected to a different AIL. In this case, a SNAC router advertising a default route may receive a packet destined for a link that is not an AIL for that router, but is an AIL for a different router. In such a case, if the infrastructure is not capable of routing between these two AILs, a packet which could have been delivered by another SNAC router will be dropped by the SNAC router that received it.

As indicated in Section 5, support for multiple AILs connected to the same stub network is out of scope of this specification. Nevertheless, to support future versions of this specification or related extensions, a SNAC router SHOULD be configurable to not advertise itself as a default router on the stub network. A SNAC router SHOULD be configurable to explicitly advertise AIL prefixes on the stub network even if it is advertising as a default router on the stub network. The mechanisms by which such configuration can be accomplished are out of scope for this document.

It is also possible that SNAC routers for more than one stub network are connected to the same AIL. In this case, the SNAC routers will be advertising Route Information Options (RIO) in their Router

Advertisement messages for their OSNR prefixes. A SNAC router MUST track the presence of such routes, and MUST advertise reachability to them on its stub network interface.

6.5. Providing discoverability between stub network links and infrastructure network links

Since DNS-SD [RFC6763] is in wide use, and provides for ad-hoc, self-configuring advertising using the mDNS transport, this is a suitable mandatory-to-implement protocol for stub networks, which must be able to attach to infrastructure networks without the help of new mechanisms provided by the infrastructure. Therefore, a SNAC router MUST provide DNS-SD service as described in this section.

6.5.1. Discoverability by hosts on adjacent infrastructure links

The adjacent infrastructure link can be assumed to already enable some service discovery mechanism between hosts on the infrastructure network, and can be assumed to provide a local DNS resolver. Therefore, this document does not define a stub-network-specific mechanism for providing these services on the infrastructure network.

In some cases it will be necessary for hosts on the AIL to be able to discover devices on the stub network. In other cases, this will be unnecessary or even undesirable. For example, it may be undesirable for devices on an AIL to be able to discover devices on a Wi-Fi tether provided by a mobile phone.

One example of a use case for stub networks where such discovery is desirable is the constrained network use case. In this case a low-power, low-cost stub network provides connectivity for IoT devices that provide services to the infrastructure. For such networks, it is necessary that devices on the infrastructure network are able to discover devices on the stub network.

The most basic use case for this is to provide feature parity with existing solutions like multicast DNS (mDNS). For example, a light bulb with built-in Wi-Fi connectivity might be discoverable on the adjacent infrastructure link to which it is connected, using mDNS, but likely is not discoverable on other links. To provide equivalent functionality for an equivalent device on a constrained network that is a stub network, the stub network device must be discoverable on the infrastructure link (which is an AIL from the perspective of the stub network).

If services are to be advertised using DNS Service Discovery [RFC6763], there are in principle two ways to accomplish this. One is to present services on the stub network as a DNS zone which can

then be configured as a browsing domain in the DNS ([RFC6763], Section 11). The second is to advertise stub network services on the AIL using multicast DNS (mDNS) [RFC6762].

Because this document defines behavior for SNAC routers connecting to infrastructure networks that do not provide any new mechanism for integrating stub networks, there is no way for a SNAC router to provide DNS-SD service on an adjacent infrastructure link in the form of a DNS zone in which to do discovery. Therefore, service on the adjacent infrastructure link MUST be provided using an Advertising Proxy, as defined in [I-D.ietf-dnssd-advertising-proxy].

One limitation of this solution is that it requires that hosts on the stub network use the DNS-SD Service Registration Protocol (SRP) [RFC9665] to register their DNS-SD services. This means that in the case of a stub network used for Wi-Fi tethering, hosts using mDNS on the stub network will not be discoverable by hosts on the infrastructure network. Any solution to this problem would require that the SNAC router provide a Discovery Proxy [RFC8766]. However, a discovery proxy is queried using DNS, not mDNS. This requires assistance from the infrastructure network, and is therefore out of scope for this document.

6.5.2. Providing discoverability of adjacent infrastructure hosts on the stub network

Hosts on the stub network may need to discover hosts on the AIL, or on the stub network. In an IoT use case, for example, there might be a light switch on the stub network which needs to be able to actuate a light bulb connected to the AIL. In order to know where to send the actuation messages, the light switch will need to be able to discover the light bulb’s address somehow.

Because the stub network is managed by SNAC routers, any DNS resolver that’s available on the stub network will necessarily be provided by one or more SNAC routers. This means that the SNAC router can enable discovery of hosts on the AIL by hosts on the stub network using a Discovery Proxy [RFC8766]. The Discovery Proxy can be advertised as available to hosts on the stub network through the DNS resolver provided on the stub network, as described in Section 11 of [RFC6763].

By implication, this means that a SNAC router MUST provide a DNS resolver. In addition, a SNAC router MUST provide a DNS zone for the AIL it is attached to, and MUST list this zone in the list of default browsing domains as defined in Section 11 of [RFC6763]. A SNAC router MUST provide a Discovery Proxy that operates with this DNS zone.

A SNAC router may provide any valid DNS zone for which it can be authoritative. However, in general the allocation and configuration of such zones is not automatic, and automatic configuration of such zones is out of scope for this document. Unless otherwise configured, a SNAC router MUST use the 'default.service.arpa' zone for this purpose.

The SNAC router MUST also maintain an SRP registrar and use registrations made through that SRP registrar to populate a DNS zone which is advertised as a default browsing domain, as defined above. Note that per Section 3.1.2 of [RFC9665] the special-use domain name 'default.service.arpa' is always available for SRP registrations into this default DNS zone. This SRP registrar MUST be advertised on the stub network either using the 'dnssd-srp' and/or 'dnssd-srp-tls' service names or some stub-network-specific mechanism, the details of which are out of scope for this document.

7. Providing reachability to IPv4-only services to hosts on the stub network

Stub networks rely on IPv6 to enable routing between links, which would not be possible with IPv4 due to the limited availability and functionality of IPv4 router discovery mechanisms (such as ICMP Router Discovery Messages [RFC1256]) compared to IPv6 Router Advertisements. However, it can still be useful for hosts on the stub network to establish communications with IPv4-only hosts on the infrastructure network or the Internet.

Although NAT64 [RFC6146] provides IPv6-only hosts with a way to reach IPv4 hosts, there is no easy way for an IPv4 host to use NAT64 to originate communication with an IPv6 host. Therefore, a SNAC router enables IPv6 hosts on the stub network to discover and reach IPv4 hosts on infrastructure, but does not provide a way for IPv4-only hosts on infrastructure to communicate to IPv6 hosts on the stub network.

This should be acceptable, because hosts on the infrastructure network that need to access stub network hosts should not be IPv4-only. A SNAC router provides IPv6 addressability on the AIL, suitable for IPv6 communication with hosts on the stub network -- infrastructure network hosts without an IPv6 stack are explicitly not in scope of this solution.

So the purpose of providing IPv4 connectivity for stub network hosts is to enable communication with arbitrary IPv4 hosts which may not be on the AIL. This is accomplished by providing NAT64 address translation in the SNAC router, and by enabling service discovery using a Discovery Proxy.

A SNAC router MUST be capable of providing NAT64 itself, and MUST be capable of discovering the availability of NAT64 service on the infrastructure network and providing it to its stub network when it is available and suitable.

Some network media may provide their own mechanisms for advertising NAT64 service to the stub network. If such a mechanism is available, a SNAC router MUST use the mechanism provided by the network medium used on the stub network to advertise NAT64 service. Otherwise, NAT64 service MUST be advertised using the PREF64 Router Advertisement option [RFC8781].

All the normative requirements in the remainder of this section (including subsections) apply to the default operation of a SNAC router. A SNAC router SHOULD be administratively configurable to disable and re-enable its NAT64 function. In case that the NAT64 function in a SNAC router is administratively disabled, these requirements do not apply as long as the NAT64 function remains disabled. Note that if NAT64 is disabled, the SNAC router's discovery and use of NAT64 service on the infrastructure network is also disabled.

There are four possible combinations of circumstances in which to consider how to provide NAT64 service:

1. Infrastructure provides DHCPv6 PD support, and the infrastructure provides NAT64

2. Infrastructure provides no DHCPv6 PD support, infrastructure provides NAT64, and there is no IPv4 on infrastructure

3. Infrastructure provides no DHCPv6 PD support, infrastructure provides NAT64, and there is IPv4 on infrastructure

4. Infrastructure provides no DHCPv6 PD support, infrastructure provides no NAT64 (and may also not be providing IPv6), and there is IPv4 on infrastructure

In the first case, infrastructure-provided NAT64 is preferred, and the SNAC router MUST advertise this NAT64 service to the stub network.

In the second case, there is no way to provide connectivity to the infrastructure network: there is no IPv6 routing other than to the adjacent infrastructure link, because there is no routable prefix, and there is no NAT64 for the same reason, and there is no IPv4, so the SNAC router can't do NAT64 on its own. In this case, the SNAC router MUST NOT advertise NAT64 service.

In the third case, despite the infrastructure network providing NAT64, nodes in the stub network can’t use it, so the SNAC router MUST provide its own NAT64 service.

In the fourth case, the SNAC router MUST provide its own NAT64 service.

An additional complication is that there may be more than one SNAC router connecting the stub network to infrastructure. In this case, it may be desirable to limit the number of SNAC routers providing NAT64 service, or it may be acceptable for all SNAC routers to provide it.

In the latter case, this should not be a problem: since each SNAC router is using its own ULA site prefix to provide NAT64, any 5-tuple that goes through a SNAC router’s NAT64 translator will necessarily have as its destination an IPv6 address in a particular NAT64 prefix, and that address will select the correct SNAC router through which to send the packet for translation. This also works on the return path, because each SNAC router has its own IPv4 address, and the return packet will be destined for that IPv4 address, and hence will always return through the SNAC router that translated it on the way out.

A further complication is that in some cases, some SNAC routers connected to the stub network may not be able to advertise an infrastructure-provided NAT64 prefix, while others may. In this case, when an infrastructure-provided NAT64 service is already advertised on the stub network, a SNAC router that was initially not able to advertise a NAT64 service on the stub network MUST stop attempting to advertise NAT64 service itself until the moment that there is no more NAT64 service advertised on the stub network.

For stub network technologies that support the advertising of a NAT64 service with an associated preference level, the below rules for preference level selection MUST be used. For stub network technologies that don’t support this (for example, technologies using the PREF64 option), these rules do not apply.

To differentiate between infrastructure-provided NAT64 service and SNAC router-provided NAT64 service, a SNAC router that advertises infrastructure-provided NAT64 service MUST use a preference of ’medium’ for this service. A SNAC router advertising its own service MUST use a preference of ’low’.

In some cases a SNAC router may be administratively configured with a NAT64 prefix. In this situation, the SNAC router MUST advertise the prefix with a preference of ’high’.

A SNAC router MUST monitor the advertisement of other NAT64 prefixes on the stub network. If a SNAC router is advertising a NAT64 prefix on a constrained stub network, and another NAT64 prefix is advertised on the stub network with a higher preference, the SNAC router SHOULD deprecate the NAT64 prefix it is advertising. This rule is based on the assumption that for a constrained stub network technology the size of the network configuration data needs to be minimized. Exceptions specific to a stub network technology may apply.

7.1. NAT64 provided by infrastructure

Stub networks are defined to be IPv6-only because it would be difficult to implement a stub network using IPv4 technology. However, stub network devices may need to be able to communicate with IPv4-only services either on the infrastructure network, or on the global Internet. Ideally, the infrastructure network fully supports IPv6, and all services on the infrastructure network are IPv6-capable. In this case, perhaps the infrastructure network provides NAT64 service to enable communication with IPv4-only hosts on the Internet. In this ideal setting, the SNAC router need do nothing— the infrastructure network is doing it all.

In this situation, if there are multiple SNAC routers, each connected to the same AIL, there is no need for special behavior— each SNAC router can advertise a default route, and any SNAC router may be used to route NAT64 traffic. If some SNAC routers are connected to different AILs than others, some of which support NAT64 and some of which do not, then the default route may not carry traffic to the correct link for NAT64 service. Advertising (on the stub network) a specific route to the NAT64 prefix would resolve this issue. However, given that support for multiple AILs connected to the same stub network is out of scope (see Section 5), there are no normative requirements related to this for a SNAC router.

In order for infrastructure-provided NAT64 to work, the stub network must have an OSNR prefix that is known to the infrastructure. Typically this means that the SNAC router must have acquired this prefix using DHCPv6 prefix delegation. Unless otherwise configured to do so, the SNAC router MUST NOT advertise infrastructure-provided NAT64 service on the stub network if the OSNR prefix was not acquired through DHCPv6 prefix delegation.

7.2. NAT64 provided by SNAC router(s)

Most infrastructure networks at present do not provide NAT64 service. Many infrastructure networks do not provide DHCPv6 prefix delegation. In these cases it is necessary for SNAC routers to be able to provide NAT64 service if IPv4 hosts are to be reachable from the stub network. Therefore, a SNAC router MUST be capable of providing NAT64 service to the stub network. When infrastructure-provided NAT64 service is not present or is not usable, and when no other NAT64 service is already advertised on the stub network, a SNAC router MUST enable its own NAT64 service and advertise it on the stub network.

To provide NAT64 service, a SNAC router MUST allocate a NAT64 prefix. For convenience, the SNAC router allocates a single prefix out of the ULA site prefix that it maintains. Out of the 2^16 possible subnets of the /48, the SNAC router SHOULD use the numerically highest /64 prefix.

If there are multiple SNAC routers providing connectivity between the stub network and infrastructure, each stub network uses its own NAT64 prefix— there is no common NAT64 prefix. The reason for this is that NAT64 translation is not stateless, and is tied to the SNAC router's IPv4 address. Therefore, each NAT64 egress is not equivalent.

This specification requires the stub network host itself to perform DNS64 [RFC6147] synthesis, as needed. A SNAC router does not provide DNS64 synthesis. Instead, it MUST provide an ipv4only.arpa answer that advertises the NAT64 prefix for that SNAC router, and MUST provide an explicit route to that NAT64 prefix on the stub network using RA or an equivalent protocol for that stub network type.

In constrained networks it can be very useful if stub network DNS resolvers provide the information required to do DNS64 translation in the answer to the AAAA query. If the answer to an AAAA query comes back with "no data" (not NXDOMAIN), this suggests that there may be an A record. In this case, the DNS resolver in the SNAC router SHOULD attempt to look up an A record on the same name. If such a record exists, the DNS resolver SHOULD return no data in the Answer section of the DNS response, and SHOULD provide any CNAME records that were involved in returning the "no data" answer to the AAAA query, and SHOULD provide any A records that were ultimately returned, in the Additional section. The response message SHOULD also include an ipv4only.arpa record in the Additional section.

8. Services Provided by a SNAC router

In order to provide network access, a SNAC router must be able to provide some network services to its stub network. In this document the following services have been discussed:

DNS Resolver: The SNAC router MUST provide a DNS resolver. If RA messages are in use on the stub network, the DNS resolver is advertised in the Router Advertisement Recursive DNS Server (RDNSS) option. If RA messages are not in use on the stub network, then the mechanism whereby the DNS resolver is advertised by the SNAC router is specific to that type of stub network.

DHCPv6 Server: The use of DHCPv6 on the stub network is NOT RECOMMENDED. In some cases it may be necessary, but should be disabled by default if the SNAC router provides this capability at all.

Discovery Proxy: In order to discover services on the AIL, a SNAC router MUST act as a Discovery Proxy on the AIL to which it is attached.

SRP Registrar: A SNAC router MUST provide SRP registrar service. This service MUST be advertised using DNS-SD in a legacy browsing domain (Section 11 of [RFC6763]) that is discoverable through the SNAC router’s DNS resolver.

Legacy Browsing Domains: The DNS resolver in the SNAC router MUST advertise a legacy browsing domain for its AIL, for the DNS zone that is maintained by its SRP service, and in addition it MUST list the legacy browsing domains provided by the infrastructure network, if any.

NAT64: A SNAC router needs to provide NAT64 service in particular circumstances so that IPv6 hosts on the stub network can communicate with IPv4 hosts on the infrastructure network and the global Internet. See Section 7.2 for detailed requirements.

9. IANA Considerations

This document updates the ’default.service.arpa’ entry in the IANA service.arpa subdomain registry by adding a second entry for that domain. The new entry has the description "default Discovery Proxy browsing domain for SNAC routers." The reference is to this document. These two uses are mutually complementary; the reason for using a second entry is to make it clear which use case is described in which document.

10. Security Considerations

Because a SNAC router operates as an IPv6 router that sends and receives IPv6 Neighbor Discovery protocol messages, the security considerations of Section 11 of [RFC4861] apply.

And because a SNAC router operates as an SRP registrar, the security and privacy considerations of Section 6 and 7 of [RFC9665] apply.

A SNAC router MUST support DNS-over-TLS as specified in Section 7 of [RFC9665] for any DNS unicast communication with hosts (acting as DNS clients) in the stub network. This provides opportunistic privacy for SRP Updates as well as for DNS queries. See [RFC7435] for the "opportunistic security" concept and Section 3.1 of [RFC7858] for the opportunistic privacy profile as defined for DNS-over-TLS. This prevents eavesdroppers on the stub network that are not able to intercept the TLS connection from determining what queries are being made. However, there is no protection against interception on the stub network other than that it may be difficult to accomplish. Support for non-opportunistic DNS-over-TLS is out of scope for this document.

There is also no guarantee that privacy-preserving DNS service will be available on the AIL. When such DNS service is present, the SNAC router SHOULD use it, if it is technically capable of doing so. However, there is no way to signal on the stub network that this is being done. Given that the privacy profile supported here is opportunistic, the DNS client has no guarantee of privacy. Aggregation of queries originating from the stub network by the SNAC router provides some degree of anonymization, but in any case because the TLS server’s certificate is not being validated by the client, the client can’t assume it is getting more privacy than an unauthenticated TLS connection can deliver.

If a SNAC router receives a DNS query protected by TLS from a stub network host, it may happen that the query is forwarded without TLS security to the upstream DNS resolver that is configured by the infrastructure network. This enables an on-path eavesdropper in the infrastructure network to observe any DNS queries that the SNAC router forwards to the upstream DNS resolver, or an on-path attacker to spoof DNS responses to such queries.

Stub network hosts that implement DNSSEC [RFC9364] can perform DNSSEC validation of DNS responses received from the DNS recursive resolver on the SNAC router.

11. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8766] Cheshire, S., "Discovery Proxy for Multicast DNS-Based Service Discovery", RFC 8766, DOI 10.17487/RFC8766, June 2020, <https://www.rfc-editor.org/info/rfc8766>.

[RFC8781] Colitti, L. and J. Linkova, "Discovering PREF64 in Router Advertisements", RFC 8781, DOI 10.17487/RFC8781, April 2020, <https://www.rfc-editor.org/info/rfc8781>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

[RFC9663] Colitti, L., Linkova, J., Ed., and X. Ma, Ed., "Using DHCPv6 Prefix Delegation (DHCPv6-PD) to Allocate Unique IPv6 Prefixes per Client in Large Broadcast Networks", RFC 9663, DOI 10.17487/RFC9663, October 2024, <https://www.rfc-editor.org/info/rfc9663>.

[RFC9665] Lemon, T. and S. Cheshire, "Service Registration Protocol for DNS-Based Service Discovery", RFC 9665, DOI 10.17487/RFC9665, June 2025, <https://www.rfc-editor.org/info/rfc9665>.

[RFC9762] Colitti, L., Linkova, J., Ma, X., Ed., and D. Lamparter, "Using Router Advertisements to Signal the Availability of DHCPv6 Prefix Delegation to Clients", RFC 9762, DOI 10.17487/RFC9762, June 2025, <https://www.rfc-editor.org/info/rfc9762>.

[RFC9915] Mrugalski, T., Volz, B., Richardson, M., Jiang, S., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", STD 102, RFC 9915, DOI 10.17487/RFC9915, January 2026, <https://www.rfc-editor.org/info/rfc9915>.

[I-D.ietf-dnssd-advertising-proxy] Cheshire, S. and T. Lemon, "Advertising Proxy for DNS-SD Service Registration Protocol", Work in Progress, Internet-Draft, draft-ietf-dnssd-advertising-proxy-04, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-dnssd-advertising-proxy-04>.

[I-D.ietf-6man-snac-router-ra-flag]
Hui, J., "SNAC Router Flag in ICMPv6 Router Advertisement Messages", Work in Progress, Internet-Draft, draft-ietf-6man-snac-router-ra-flag-06, 8 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-snac-router-ra-flag-06>.

12. Informative References

[RFC1256] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, DOI 10.17487/RFC1256, September 1991, <https://www.rfc-editor.org/info/rfc1256>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/info/rfc4944>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[Tethering] Wikipedia, "Tethering", March 2026, <https://en.wikipedia.org/w/index.php?title=Tethering&oldid=1343931068>.

[Thread] Thread Group, "Thread 1.4.0 Specification", September 2024, <https://www.threadgroup.org/ThreadSpec>.

Appendix A. Analysis of deployment scenarios in which a SNAC router could cause problems

This appendix is informative.

A.1. Unmanaged home network

In this scenario, a non-expert home user connects a SNAC router to their own unmanaged home network. This is the key intended use case for stub networks. This document describes how to implement a SNAC router such that it operates correctly in this situation, whether the ISP is providing IPv6 reachability to the Internet or not.

In some unmanaged network settings, there is a "guest" network in addition to the main network. In this configuration, if a SNAC router is added to the guest infrastructure network, no communication between that router’s stub network and other nodes in the home will be possible. The general intended behavior of the guest network is to isolate untrusted hosts. Since this would be the intended behavior on the part of the owner of the network, it won’t be a surprise to them, since they had to explicitly give the SNAC router’s owner the guest network credentials and not the main network credentials. This should also mean that the owner of the SNAC router will not expect it to fully function in this scenario.

An additional feature of some unmanaged networks is that the owner of the network can choose to isolate all devices on the network, so that devices on the network are able to use the Internet, but not communicate with each other. In this case, one can assume that the owner of the network doesn't expect any devices attached to the network to be able to communicate with any other device, so the failure of devices connected to infrastructure to communicate with devices on the stub network would not be a surprise. The owner of the SNAC router might be surprised in this case, but ultimately the owner of the infrastructure network gets to make this decision, and there isn't anything a SNAC router can or should do on behalf of the SNAC router's owner in this case.

A.2. Use on an unmanaged (non-home) IPv6 network

In this scenario there is a site that is not a home, so perhaps a restaurant or business, where there is no network operator per se, and the network is deployed similarly to a home network. There is little difference between this scenario and an unmanaged home network, but expectations may be different. In particular, it is very common in such settings for there to be a guest network for visitors, or for the network to enforce isolation between all nodes connected to it.

A.3. Use on a managed network

In this scenario, a non-expert user attaches a SNAC router to an infrastructure network that's managed and provides both IPv6 and IPv4. This network has correctly deployed RA Guard and/or port-based access control. As a result, the SNAC router won't succeed in advertising a prefix on the managed network. Communications originating on the stub network that are able to communicate using NAT64 will still work.

In the managed network case, it's possible that the network operator is willing to permit SNAC routers to be attached to the network by users. In this case, they might either not deploy RA guard, or they might deploy working DHCPv6 prefix delegation. This could be PD-per-host (where hosts are encouraged to use prefix delegation) or just ordinary prefix delegation (where hosts are given prefix delegation if they ask for it, but not encouraged to ask for it).

In such a situation, if DHCPv6 PD works on the adjacent infrastructure link, the SNAC router will function correctly, because the delegated prefix will be correctly routed.

It’s worth noting that IPv4 devices that act similarly to SNAC routers, using NAT64, already exist and may indeed use the stub network functionality to support internal connections that aren’t even apparent to the user. In this case the SNAC router is not relying on RA to function because it’s using its IPv4 address and NAT64 to provide connectivity, so there is no management issue even if RA is blocked. This is a reasonable use case for IPv6, and this specification does in fact enable this use case.

When a SNAC router is attached to an infrastructure network that has deployed RA guard and does not support DHCPv6 prefix delegation, and where that infrastructure network does allow the use of multicast DNS, services advertised on the stub network will be discoverable on the infrastructure network, but will not be reachable.

A.3.1. Managed networks where DHCPv6 is required but RA guard is not present

There can be a case where an infrastructure network does not implement RA guard, does not advertise what a SNAC router considers to be a "suitable" prefix, and does provide addressing using DHCPv6 IA_NA. In this situation, it could be the case that two ULA prefixes are being advertised as on-link on the AIL and one is being advertised as permitting autonomous address configuration. The latter is the ULA on-link prefix being provided by a SNAC router.

In case a host on the AIL attempts to communicate with a device using a site ULA prefix on a different link, it may choose a ULA address as its source address. If it were to choose the autonomously-configured ULA address as its source address, this would fail, because there is no route back from the different link to the SNAC-router-provided ULA prefix.

However, this can only happen in practice if the host did not receive an address from DHCPv6. In this case, the host would not be able to communicate anyway. The problem that might occur here is that a series of IPv6 packets with an unexpected source address are sent to a device on another link, and that device would be unable to send a response.

In such scenarios there is no way to actually know based on the network configuration what the operator’s intention was. An operator that sees a problem with this can react by implementing RA guard or by blocking unknown source addresses at the router, and in so doing they would be expressing their intention. This configuration would not cause any new problem: a host that could communicate would still be able to communicate, and a host that could not communicate would not become able to communicate.

The one scenario where a communication problem can actually be expected is when there is a GUA prefix advertised by infrastructure but no ULA prefix, but there is a ULA destination to reach. In this case, the longest-matching-prefix algorithm could choose the SNAC-router-provided ULA prefix as a source address to reach the site-provided ULA destination, and in this case communication would fail. Only "Happy Eyeballs" [RFC8305] can correct this situation.

A.3.2. Use on a managed network without IPv6

In this scenario, there is no IPv6 service being intentionally advertised on a managed network. Operators of such networks may not be aware of the possibility of configuring RA guard. In this situation, a SNAC router will connect and advertise services, which will be reachable just as they would be in a similar unmanaged network. A SNAC router that conforms to this specification will not advertise an IPv6 default route on any interface. Therefore, it should not cause operational problems, just as connecting an IPv4 NAT gateway in the same scenario would not cause operational problems.

Appendix B. Router Advertisements on the Infrastructure Network

This appendix is informative only. Any values provided here are based on the normative requirements in this document, [RFC4861] and other referenced documents.

An active SNAC router sends periodic unsolicited multicast Router Advertisements as well as unicast Router Advertisements on the adjacent infrastructure link. These Router Advertisements are filled with the following values consistent with the message format given in Section 4.2 of [RFC4861]:

* Router Lifetime: A SNAC router never advertises itself as a default router on infrastructure. Therefore, the router lifetime is always zero in a SNAC router’s Router Advertisements sent on the AIL.

* For the ’M’ and ’O’ flag bits, Section 6.1.2.3 specifies how the values are set. In case that no other router (excluding SNAC routers) on the AIL has set these flags, they are both set to zero.

* The ’SNAC router’ flag ([I-D.ietf-6man-snac-router-ra-flag]): 1

* In the Cur Hop Limit field: 0 ("unspecified by this router")

* In the Reachable Time field: 0 ("unspecified by this router")

* In the Retrans Timer field: 0 ("unspecified by this router")

* In the options:

  - Source Link-Layer Address option: Including this option whenever possible is recommended. The load balancing use case in Section 6.2.3 of [RFC4861] is out of scope for this document and is not generally expected to be applicable. The benefit of including this option is that it eliminates the need to do Neighbor Discovery on the SNAC router's link-local address to get its link-layer address.

  - MTU option: the SNAC router is not managing the link, and hence should not send this option.

  - Prefix Information options: when there is no suitable prefix (See Section 6.1.1) on the adjacent infrastructure link, some SNAC router will need to send a PIO. However, unless they are able to cooperate in choosing a PIO, only one SNAC router will send a PIO. How this decision is made is described in Section 6.1.2. When a SNAC router sends this option, the following settings apply:

    o In the 'L' flag bit (on-link): 1

    o In the 'A' flag bit (autonomous address configuration): 1

    o In the Valid Lifetime field: normally STUB_PROVIDED_PREFIX_LIFETIME, but see Section 6.1.2.5.

    o In the Preferred Lifetime field: normally STUB_PROVIDED_PREFIX_LIFETIME, but see Section 6.1.2.5.

  - Route Information Option: an active SNAC router always provides a Route Information Option for each OSNR prefix that is valid on the stub network. This provides a route from the infrastructure network to the stub network. The following settings apply:

    o Prefix Length: 64

    o Route Preference: low

    o Route Lifetime: the remaining valid lifetime of the OSNR prefix on the stub network, but no more than STUB_NETWORK_ROUTE_LIFETIME

    o Prefix: the OSNR prefix advertised on the stub network

- Any other RA options: a SNAC router does not send any further RA options, because the SNAC router is not responsible for managing the infrastructure network.

Per Section 6, all RA options for a SNAC router must fit in a single RA message. SNAC routers do not send multiple RAs with different information other than to announce that some information that was previously advertised has changed.

Appendix C. Router Advertisements on the stub network

This appendix is informative only. Any values provided here are based on the normative requirements in this document, [RFC4861] and other referenced documents. This appendix is only applicable to stub network technologies that support sending of IPv6 ND Router Advertisement messages in the format defined by [RFC4861]. Note that this is typically not the case for 6LoWPAN-based stub network link-layer technologies.

A SNAC router sends unsolicited periodic as well as solicited Router Advertisements on its stub network interface, filled with the following values consistent with the message format given in Section 4.2 of [RFC4861]:

* Router Lifetime: The SNAC router can be a default router on the stub network (see Section 6.4). In this case, the value is the remaining lifetime of the default route that was detected on the AIL with a maximum of STUB_NETWORK_ROUTE_LIFETIME. If it is not a default router, the value is zero.

* SNAC routers do not provide DHCP service on the stub network. Therefore, the ’M’ and ’O’ flag bits must be zero.

* The ’SNAC router’ flag ([I-D.ietf-6man-snac-router-ra-flag]): 0. Note that this flag is only set by the SNAC router in RA messages sent on its AIL interface.

* In the Cur Hop Limit field: 0 ("unspecified by this router")

* In the Reachable Time field: 0 ("unspecified by this router")

* In the Retrans Timer field: 0 ("unspecified by this router")

* In the options, the SNAC router may send options as appropriate.

  - Source Link-Layer Address option: Including this option whenever possible is recommended. The load balancing use case in Section 6.2.3 of [RFC4861] is out of scope for this document

and is not generally expected to be applicable. The benefit of including this option is that it eliminates the need to do Neighbor Discovery on the SNAC router's link-local address in order to get its link-layer address.

- MTU option: the SNAC router is managing its stub network link, and hence may send this option.

- Prefix Information option: Some SNAC router will need to send a PIO. Normally, only one SNAC router on the same stub network will send a PIO. How this decision is made is described in Section 6.2. When a SNAC router sends this option, the following settings apply:

  - In the 'L' flag bit (on-link): 1

  - In the 'A' flag bit (autonomous address configuration): 1

  - In the Valid Lifetime field: normally STUB_PROVIDED_PREFIX_LIFETIME, but see Section 6.1.2.5.

  - In the Preferred Lifetime field: normally STUB_PROVIDED_PREFIX_LIFETIME, but see Section 6.1.2.5.

- Route Information Option: when a SNAC router is not advertising a default route, it must include one or more RIO options in Router Advertisement messages on the stub network to provide reachability to infrastructure. This is discussed in Section 6.4. The following settings apply:

  - Prefix Length: the length of the prefix covered by the route, not necessarily 64.

  - Route Preference: low

  - Route Lifetime: The lifetime of the on-link prefix on the AIL, or route lifetime of the route observed on the AIL, but no more than STUB_NETWORK_ROUTE_LIFETIME

  - Prefix: the prefix that is known to be reachable on the infrastructure network

Appendix D. Handling failure and change situations on a stub network

How a SNAC router handles situations of device failure, network failure or other changes on its stub network is outside the scope of the normative specification for a SNAC router. This handling depends on the specific stub network technology being used. This informative appendix provides guidance about the expected behavior and properties of the stub network with respect to failure and change situations, such that the interoperability goals (Section 1.1) and the usability goals (Section 1.2) can be satisfied.

A SNAC router that supports cooperation between multiple SNAC routers in the same stub network is expected to support the following basic failure and change situations by automatically adapting to the new situation:

* A new SNAC router is added to the stub network.

* A SNAC router is powered down, or removed from the stub network.

* An existing SNAC router is powered up again, after a short (e.g. reboot) or long period of time.

* A SNAC router fails and stops operating.

* Connectivity in the stub network changes due to e.g. changing radio conditions, moved devices, or plugged/unplugged cables.

While the details of how a stub network technology supports these basic cases is out of scope of this document, some hints, suggestions and examples from current stub network technologies are discussed below.

Some technologies used for stub networks, for example Thread or 6LoWPAN wireless mesh networks, can produce partitioned networks, where what is notionally the same stub network winds up looking like two or more discrete links. Such partitions can form and rejoin over time as a result of either changes in radio propagation or the addition of, or removal of, or mobility of, devices on the mesh.

On stub networks that can partition, one way of detecting that a partition has occurred is to notice that the SNAC router that has advertised the on-link OSNR prefix for the stub network is no longer reachable via the stub network. A SNAC router that notices such a loss of reachability can take action in order to satisfy the requirement in Section 6.2 that at least one SNAC router provides an OSNR prefix. How this requirement is satisfied is specific to the stub network technology used. For example, the SNAC router could

autonomously decide to advertise its own OSNR prefix if it sees that no other SNAC router is advertising an OSNR prefix yet. Or, it could perform a coordination protocol with the other SNAC routers that it can still reach, to determine which of the SNAC routers should provide the OSNR prefix next.

An implication of this is that when such a partition forms, the same OSNR prefix cannot be advertised on both partitions, since this will result in ambiguous routing to/from the infrastructure network. This problem is already addressed by the requirement that each SNAC router generate its own ULA site prefix (see Section 6.2.1), from which a unique ULA OSNR prefix is allocated.

When partitions of this type occur, they may also heal at a later time. When a stub network heals in a situation where two SNAC routers have both been advertising an OSNR prefix on their respective partitions, it will now appear that there are two OSNR prefixes on the same stub network.

How the case of two or more OSNR prefixes on the same stub network is handled, is specific to the stub network technology. Some technologies may easily handle multiple OSNR prefixes, while other more constrained network technologies may need to apply a maximum to the number of OSNR prefixes for resource/efficiency reasons. See Section 6.2.2 for more discussion on such single-prefix and multiple-prefix constraints. While that section has DHCPv6-specific requirements only, the general issue needs to be resolved by a stub network technology also for deployments in which DHCPv6-PD is not available or deployments with mixed DHCPv6/ULA based OSNR prefixes.

As an example that can be used in a constrained stub network: a feasible strategy is for each SNAC router to perform a numeric comparison between the multiple OSNR prefixes and let the numerically lowest prefix/prefixes "win". The prefixes that don’t win are deprecated. This has the benefit that non-ULA DHCPv6-PD delegated OSNR prefixes are selected in favor of the numerically higher ULA link prefixes, thus supporting the SNAC interoperability goal of IP connectivity to the Internet.

Authors’ Addresses

Ted Lemon
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America
Email: mellon@fugue.com

Jonathan Hui
Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043
United States of America
Email: jonhui@google.com

Esko Dijk
IoTconsultancy.nl
Utrecht
Netherlands
Email: esko.dijk@iotconsultancy.nl