v6ops
Internet-Draft
Intended status: Best Current Practice
Expires: 22 April 2026

J. Palet Martinez
The IPv6 Company

19 October 2025

IPv6 Prefix Assignment to end-users
draft-palet-v6ops-prefix-assignment-00

Abstract

This document describes different alternatives and best current practices for assignment of IPv6 prefixes for end-user broadband networks, including considerations about point-to-point links, their size, numbering choices, pool choices, customer prefix assignment size and persistance of those assignments.

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 22 April 2026.

Table of Contents

1. Introduction

When deploying IPv6 in broadband networks to end-users (both residential and enterprise), there are different alternatives to tackle the most common open questions:

* What size for the point-to-point links?

* How to number the point-to-point links?

* What pool to use for the point-to-point links?

* What prefix size should be assigned to customers?

* Should the customers prefixes be persistent?

From an operational perspective, each choice may have different advantages or disadvantages that need to be taken in consideration under the scope of each specific network architecture design, as already described in the RIPE BCOP 690 document [RIPE-690] that has been extensively used across many years.

For example, [RFC6164] describes using /127 prefixes for inter-router point-to-point links, using two different address pools, one for numbering the point-to-point links and another one for delegating the prefixes at the end of the point-to-point link. However, this doesn’t exclude other choices.

The proposed approaches are suitable for those point-to-point links connecting ISP to customers, but not limited to those cases, and in fact, all them are being used by a relevant number of networks worldwide, in several different scenarios (service providers, enterprise networks, etc.).

This document describes the best current practices for each of those different aspects.

Note that across this document, we can use interchangeably end-user, customer, subscriber or end-site, as what it actually matters is what is connected behind an individual link.

2. Requirements Language

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.

3. Point-to-Point Links Considerations

3.1. The Ping-Pong Problem in Point-to-Point Links

Some point-to-point links may present the ping-pong problem, (a forwarding loop). The fundamental root cause of this problem is an IPv6 implementations not performing full Neighbor Discovery (NS/NA) on addresses that the prefix says could exist on the link.

IPv6 implementations are assuming that all addresses within the prefix must exist at the other end of the point-to-point link, and send the traffic straight onto the link. If the address doesn’t exist, and there is a covering route back in the other direction, the ping-pong problem occurs.

Full Neighbor Discovery is doing more than just resolving the link-layer address of an IPv6 address. Neighbor Discovery is also determining if the address exists. Even if a point-to-point link doesn’t have link-layer addresses to resolve, ND determining if an address exists on the link is very beneficial because it will prevent the ping-pong problem occurring entirely regardless of the IPv6 prefix length being used on the link.

3.2. Prefix Size Choices

[RFC7608] already discusses about the IPv6 prefix length recommendations for forwarding, and the need for routing and forwarding implementations to ensure that longest-prefix-match works on any prefix length. So, in this document, we concentrate in the most commonly used choices, not excluding other options.

3.2.1. Rationale for using /64

The IPv6 Addressing Architecture ([RFC4291]) specifies that all the Interface Identifiers for all the unicast addresses (except for 000/3) are required to be 64 bits long and to be constructed in Modified EUI-64 format.

The same document also mandates the usage of the predefined subnet-router anycast address, which has cleared to zero all the bits that do not form the subnet prefix.

Using /64 is the most common scenario and currently the best practice by the number of service providers using this approach compared to others.

Using a /64 has the advantage of being future proof and avoids renumbering, in the event that new standards take advantage of the 64 bits for other purposes, or the link becomes a point-to-multipoint, or there is a need to use more addresses in the link (e.g., monitoring equipment, managed bridges).

It has been raised also the issue of some hardware having limitations in using prefixes longer then /64, for example using extra hardware resources.

Section 5. of [RFC6164] describes possible issues when using /64 for the point-to-point links, such as the ping-pong and the neighbor cache exhaustion. However, it also states that they can be mitigated by other means, including the latest ICMPv6 [RFC4443] ND [RFC4861]. Indeed, considering the publication date of that document, those issues should not be any longer a concern. The fact is that many operators worldwide, today use /64 without any concerns, as vendors have taken the necessary code updates.

Consequently, we shall conclude that it is a valid and recommended approach to use /64 prefixes for the point-to-point links.

3.2.2. Rationale for using /127

[RFC6164] already do a complete review of reasons why /127 is a good approach vs other options. However, it needs to be considered that it was published a number of years ago, and most of the hardware today already incorporate mitigations.

It should be noted that, when using a /127 prefix, configuration of each of the addresses within the /127 prefix, at each respective end of the link, must be actively validated by the network operator. A missing /127 address from one end of the link, with a local route pointing out that end of the link that covers the missing /127 address, such as a default route, causes a "ping-pong" scenario to exist for the missing /127 address. The link could still be successfully carrying transit traffic, and IPv6 will not report any errors, because IPv6 doesn’t require, neither will check, that all interfaces attached to a link have addresses from all prefixes assigned to the link, excepting the Link-Local prefix per [RFC4291].

It is a valid approach to use /127 for the point-to-point links, however is not future proof neither recommended considering the comments from the previous section, and older equipment may not support it.

3.2.3. Rationale for using /126 and Other Options

/126 was considered by [RFC3627], and despite this document has been obsoleted, because was considering /127 as harmful, the considerations in Section 4.3 are still valid.

The same document describes options such as /112 and /120, and all those are commonly used in worldwide IPv6 deployments [IPv6-Survey], though in a lesser degree than /64 or /127.

Consequently, we shall conclude that even /126, /120 and /112 are valid approaches for the point-to-point links, are not recommened.

3.2.4. A Possible Middle-Term Choice

A possible "middle-term" approach, will be to allocate a /64 for each point-to-point link, but use just one /127 out of it, making it future proof and at the same time avoiding possible issues indicated in the previous sections. This will be also consistent with the recommendations of [RFC6583] to prevent ND operational implications.

3.3. Numbering Choices

IPv6 provides different unicast addressing scopes which can be considered when numbering a point-to-point link.

It has been reported that certain hardware may consume resources when using numbered links. This is a very specific situation that may need to be consider on a case by case basis.

3.3.1. GUA (Global Unicast Addresses)

Using GUA is the most common approach. It provides full functionality for both end-points of the point-to-point link and consequently, facilitates troubleshooting, so it is the recommended approach.

3.3.2. ULA (Unique Local Addresses)

Some networks use ULAs for numbering the point-to-point links. This approach may cause numerous problems when carrying Internet traffic and therefore, is strongly discouraged. For example, if the CE needs to send an ICMPv6 message to a host outside that network (to the Internet), the packet with ULA source address will not get thru and PMTUD will break, which in turn will completely break that IPv6 connection when the MTU is not the same for all the path.

ULAs may be considered as IPv6 private addresses, not intended to be used as source or destination addresses across the Internet. This issue also exists in IPv4 when using [RFC1918] addresses on links carrying IPv4 Internet traffic. [RFC6752] discusses this issue for IPv4, with much of the discussion applying similarly to IPv6 and ULAs.

However, this approach is valid if, following Section 2.2 of [RFC4443], and despite using ULA for the point-to-point link, the router is configured with at least one GUA and the source of the ICMPv6 messages are always a GUA, per the IPv6 Default Address Selection algorithm [RFC6724]. Consequencly, should not be recommended and might only be used in cases where the CE is provided by the service provider, specifically supports this option, and can’t be replaced by the end-user.

3.3.3. Link-Local Addresses Only

Some networks leave the point-to-point links with only Link-Local addresses used at both ends of the link. This is sometimes improperly referred as "unnumbered", because the Link-Local addresses are also "numbers". Furthermore, [RFC4291] requires that all interfaces attached to a link have at least a Link-Local "number" or address from the Link-Local prefix.

[RFC7404] (Using Only Link-Local Addressing inside an IPv6 Network) discusses pros and cons of this alternative, which in general apply for the point-to-point links.

While this choice might work if the point-to-point link is terminated in a router, which typically will get configured with a suitable routable GUA or ULA, it will not work for devices that can’t be further configured, for example if they do not support DHCPv6-PD [RFC8415]. This is the case for hosts, when the Operating System is not expected to be a DHCPv6-PD client and are therefore left without any usable GUA to allow traffic forwarding.

In the case of a router, the route for the assigned prefix is pointed towards the link-local address on the router WAN port and the default route on the router is pointed towards the link-local address on the upstream network equipment port.

This choice seems easier to implement, compared the previous ones, but it also brings some drawbacks, such as difficulties with troubleshooting and monitoring. For example, link local addresses do not appear in traceroute, so it makes more difficult to locate the exact point of failure.

It is more useful in scenarios where it is known that only a router will be attached to the point-to-point link, and where the configured address of the router is known. Non-routers connecting to a network, which can’t initiate DHCPv6-PD might experience problems and will stay unnumbered upon connection, if a /64 prefix is not used to number the link. This may be also the case for routers, which will not be able to complete the DHCPv6-PD in unnumbered links.

The considerations indicated in the previous section, regarding not using ULA as source address of ICMPv6 messages, and instead ensuring there is at least one GUA configured for that, also apply if link-locals are used for the point-to-point link. So once more, this approach is not recommended.

3.4. Prefix Pool Considerations

The logic choice seems to use a dedicated pool of IPv6 addresses, as this is the way we are "used to" with IPv4. Actually, this is done often by means of different IPv6 pools at every PoP in a service provider network.

However, this is not neccesarily the best choice. The fact that the default IPv6 link size is /64 and commonly multiple /64s are assigned to a single customer, provides an interesting alternative approach for combining best practices described in the precedent sections.

3.4.1. /64 from Dedicated Pool for point-to-point links

Using a /64 prefix from a dedicated pool of IPv6 prefixes is very common. A separate block of IPv6 space is allocated for the WAN links to the end customer CEs, so that when CE connects to the network and performs router discovery, a /64 prefix is used to number both ends of the connection.

In the case of an end-user host (not router) connected using technologies such as PPPoE, the setup process is concluded when the host is properly IPv6 numbered and can start sending and receiving traffic.

It is more common when a CE is available, as if it is capable of issuing a DHCPv6-PD request, the IPv6 prefix delegation process starts and an IPv6 prefix is assigned to the CE.

A possible benefit of using a dedicated IPv6 pool, is that allows applying security policies without harming the customers. This is only true if customers always have a CE at their end of the WAN link.

3.4.2. /64 from Customer Prefix for point-to-point links

Using a /64 from the customer prefix, in addition to the advantages already indicated when using /64, simplifies the addressing plan and storage needs for logging the addresses of the end-sites.

The use of /64 also facilitates an easier way for routing the shorter aggregated prefix into the point-to-point link. Consequently it simplifies the "view" of a more unified addressing plan, providing an easier path for following up any issue when operating IPv6 networks and typically, will have a great impact in saving expensive hardware resources (lower usage of TCAM, typically by half).

This mechanism would not work in broadcast layer two media that rely on ND, because it will try ND for all the addresses within the shorter prefix that is being routed thru the point-to-point link.

3.4.2.1. Numbering Interfaces

Often, in point-to-point links, hardware tokens are not available, or there is the need to keep certain bits (u, g) cleared, so the links can be manually numbered sequentially with most of the bits cleared to zero. This numbering makes as well easier to remember the interfaces, which typically will become numbered as 0 (with 63 leading zero bits) for the provider side and 1 (with 63 leading zero bits) for the customer side.

Using interface identifiers as 0 and 1 is not only a very simple approach, but also a very common practice. Other different choices can as well be used as required in each case.

On the other hand, using the EUI-64, makes it more difficult to remember and handle the interfaces, but provides an additional degree of protection against port (actually address) scanning as described at [RFC7707].

3.4.2.2. Routing Aggregation of the Point-to-Point Links

Following this approach and assuming that a shorter prefix is typically delegated to a customer, for example a /48, it is possible to simplify the routing aggregation of the point-to-point links. Towards this, the point-to-point link may be numbered using the first /64 of the /48 delegated to the customer.

Let’s see a practical example:

* A service provider uses the prefix 2001:db8::/32 and is using 2001:db8:aaaa::/48 for a given customer.

* Instead of allocating the point-to-point link from a different addressing pool, it may use 2001:db8:aaaa::/64 (which is the first /64 subnet from the 2001:db8:aaaa::/48) to number the link.

* This means that, in the case the non-EUI-64 approach is used, the point-to-point link may be numbered as 2001:db8:aaaa::1/64 for the provider side and 2001:db8:aaaa::2/64 for the customer side.

* Note that using the first /64 and interface identifiers 1 and 2 is a very common practice. However other values may be chosen according to each case specific needs.

In this way, as the same address pool is being used for both, the prefix and the point-to-point link, one of the advantages of this approach is to make very easy the recognition of the point-to-point link that belongs to a given customer prefix, or in the other way around, the recognition of the prefix that is linked by a given point-to-point link.

For example, making a trace-route to debug any issue to a given address in the provider network, will show a straight view, and it becomes unnecessary one extra step to check a database that correlate an address pool for the point-to-point links and the customer prefixes, as all they are the same.

Moreover, it is possible to use the shorter prefix as the provider side numbering for the point-to-point link and keep the /64 for the customer side. In our example, it will become:

* Point-to-point link at provider side: 2001:db8:aaaa::1/48

* Point-to-point link at customer side: 2001:db8:aaaa::2/64

This provides one additional advantage as in some platforms the configuration may be easier saving one step for the route of the delegated prefix (no need for two routes to be configured, one for the delegated prefix, one for the point-to-point link). It is possible because the longest-prefix-match rule.

The behavior of this type of configuration has been successfully deployed in different operator and enterprise networks, using commonly available implementations with different routing protocols, including RIP, BGP, IS-IS, OSPF, along static routing, and no failures or interoperability issues have been reported.

3.4.2.3. DHCPv6 Considerations

When using DHCPv6 [RFC8415], the Prefix Exclude Option for DHCPv6-based Prefix Delegation ([RFC6603]), allows the usage described above.

Moreover, [RFC3769] has no explicit requirement that avoids the approach described in this document.

Note that if instead of DHCPv6, other configuration means are being used, it is also possible to use a /64 from the customer allocated prefix for the point-to-point link.

3.4.2.4. Router Considerations

This approach is being used by operators in both, residential/SOHO and enterprise networks, so the routers at the customer end for those networks MUST support [RFC6603] if DHCPv6-PD is used.

In the case of Customer Edge Routers there is a specific requirement ([RFC7084]) WPD-8 (Prefix delegation Requirements), marked as SHOULD for [RFC6603]. However, in a scenario where the approach described in this document is followed, together with DHCPv6-PD, the CE Router MUST support [RFC6603].

4. Prefix Assignment to End-Users

When deploying IPv6, compared with IPv4, several new aspects need to be considered:

1. A service provider doesn’t have scarcity of IPv6 addresses, needs to think big when planning, which in turn will facilitate operations and avoid renumbering.

2. All the RIR policies permit assignments of a /48 per site and allow to obtain the prefix size according to each service provider needs, depending on their own justified need based on addressing plans.

3. To keep addressing plans usable and understandable and to align with DNS reverse zone delegations, the size of the delegated prefix should align with a nibble boundary.

4. IPv6 default prefix lengh is /64 and must not be broken down, ir order to avoid all kind of unexpected consecuences and interoperability issues.

5. There is no NAT in IPv6, as there is no need for it.

6. It is expected that each customer is able to have more than sufficient subnets as may be needed, not just at the time being, but also in the near future.

7. Following [RFC7934], [RFC8273], [RFC9762] and [RFC9663], it is a good practice to allocate to each end-device no just a single IPv6 address per interface, but instead a complete /64 prefix in each interface, allowing the seamless support of features such as containers or virtual machines, among others.

8. As end-user networks keep growing, they become more complex and in IPv6 they contain multiple chained stub networks [RFC9818].

9. As a consecuence, it is expected that each customer gets n x /64 (not just a single /64), being "n" sufficiently big, for actual and future needs.

10. In summary, IPv6 is not the same as IPv4 and consequently previous IPv4 best practices are not, in general, the best advise.

Considering the above premises, it is very clear that assigning to end-users a single /64 must be avoided at all means.

The next possible choice will be a /60, which leaves only 16 /64s available (and one of them may be used for the point-to-point link). Clearly insuficiente for enterprises even for small/medium ones, and in general, considering smart homes, this will be become clearly too small in the very near future, and must be avoided as well.

4.1. /48 for every end-user

The existing RIR policies for IPv6 allocation, allow to obtain by default at least a /32 basically without any justification. In some cases, such as in RIPE NCC, you can get a /29 also without any justification. A /32 contains 65.535 /48s, so even assuming some of those /48s lost because the network infrastructure, hierarchy, routing and so on, we can calculate a worst case where a minimum of 50.000 /48s will become available for customers.

Obviously a bigger service provider will need a bigger prefix, for example a provider with 100.000 customers will need a /31 instead of a /32, a provider with 200.000 customers will need a /30, and so on. It should be clear that, as indicated already, all the RIR policies are consistent with this, which means that if you have more customers and you decide to provide a /48 for each end-user or end-site, you are able to obtain whatever prefix size you need.

Basically, this means that there is no any practical reason to not assign /48s for every end-site, which in existing studies shows that is what is being done by a majority of service providers worldwide.

This has several advantages worth to mention:

1. It match with the minimum IPv6 prefix routable in Internet.

2. It match with the ULA prefix size.

3. It macth with the prefix size used by transition mechanisms.

4. It match with the standard direct assignment from RIRs to end-sites (Provider Indepentent, also called portable addresses).

Keeping this matching facilitates possible network changes, exchanging service providers or moving to Provider Independent addresses, all that with a direct mapping of existing addressing plans of the end-site that obtained a prefix delegation. At the same time, from the perspective of the service provider having a flat addressing plan, with the same delegated prefix size for all the customers it is clearly a big advantage, in terms of operations, monitoring, avoiding mistakes and much less call-centre time to sort out problems.

An example of this, if we consider a service provider that got 2001:db8::/32 and for a given PoP is delegating prefixes out of 2001:db8:1000::/36, the 4.096 customers in this PoP will get:

* 2001:db8:1000::/48

* 2001:db8:1001::/48

* 2001:db8:1002::/48

* 2001:db8:1003::/48

* ...

* 2001:db8:1fff::/48

In this case, the end-users are able to use for their internal addressing plans the bits marked as "X" in the addressing space of 2001:db8:1000:XXXX::/48.

In summary, a /48 is the strongly recommended best current practice for prefix size assignments to end-users.

4.2. /48 for business customers and /52 or /56 for residential customers

Some operators prefer, even if this increase their OPEX, to differentiate between business and residential customers. This rationale is understood to be mainly coming from sales and marketing departments where they wish to create some distinction in services between different types of customer. This method can be considered as pragmatic, future-proof and has nearly no downsides.

However it has implications for the customers, such as the lost of "matches" indicated in the previous section, which means that if a customer already has an addressing plan, they will be forced to redo it and renumber in case of a different prefix size. Instead, using the same prefix size, allow them to keep the addressing plan and just replace some of the prefix bits rather than have a complete numbering plan change. Note that in many cases, SMEs may be using residential services.

For more advanced customers or SMEs that manually configure their servers and infrastructure, local addressing is a bit harder for /52 or /56 prefixes, as you are unable to use all 4 digits between the double colons in the address notation. This means that there is a higher risk of making mistakes whilst making the addressing plans and sub-assign addresses to devices outside the assigned prefix. This should not be a problem in simple cases where a CE assigns all prefixes, but it might cause annoyances for those advanced users that may need to offer content and services from their own networks.

A /56 only provides 256 subnets to customers, while a /52 is providing 4.096 subnets. Even if 256 seems to be sufficient for most of the cases, if you start considering that many devices will be requiring a /64 per interface, then it quickly becomes too short. So if the reason for not providing /48 to each end-site is the differentiation among business and residential customers, the choice of /52 seems much safer in terms of future proof and maintains that differentiation factor.

Using the same example as in the previous section, if we consider a service provider that got 2001:db8::/32 and for a given PoP is delegating prefixes out of 2001:db8:1000::/36, then there will be space for 65.536 customers:

* 2001:db8:1000:0000::/52
* 2001:db8:1000:1000::/52
* 2001:db8:1000:2000::/52

* 2001:db8:1000:3000::/52

* ...

* 2001:db8:1fff:f000::/52

In this case, the end-users are able to use for their internal addressing plans the bits marked as "X" in the addressing space of 2001:db8:1000:0XXX::/52.

Once more, using the same example, considering a service provider that got 2001:db8::/32 and for a given PoP is delegating prefixes out of 2001:db8:1000::/36, the 1.048.576 customers in this PoP will get:

* 2001:db8:1000:0000::/56

* 2001:db8:1000:0100::/56

* 2001:db8:1000:0200::/56

* 2001:db8:1000:0300::/56

* ...

* 2001:db8:1fff:ff00::/56

In this case, the end-users are able to use for their internal addressing plans the bits marked as "X" in the addressing space of 2001:db8:1000:00XX::/56.

An alternative is to reserve a /48 for residential customers, but actually assign them just the first /52 or /56. If subsequently required, they can then be upgraded to the required prefix size without the need to renumber, or the spare prefixes can be used for new customers in the same PoP. Note that this only makes sense in case of IPv6 exhaustion, as obtaining a bigger allocation from the relevant RIR seems feasible accordig to existing policies and the actual trends on policy development.

4.3. Prefixes longer than /56

It is strongly discouraged to assign prefixes longer than /56 unless there are very strong and unsolvable technical reasons for doing this.

There are enough IPv6 addresses to delegate end-users a /48, so a /52 or /56 already represents a sizeable restriction Just to give an idea about order of magnitude, there are 1.048.576 /52s in a /32. There

is no need to delegate fewer addresses than that, so if your IPv6 allocation is insufficient to provide a /52 or /56 to each end-site, explain to your RIR that your initial allocation was too small and that you require a larger allocation based on your IPv6 implementation plan.

Assigning a /64 or longer prefix does not conform to IPv6 standards and will break functionality in customer LANs. With a single /64, the end customer CE will have just one possible network on the LAN side and it will not be possible to subnet, assign VLANs, alternative SSIDs, or have several chained routers in the same customer network as indicated by [RFC9818], etc.

Some CEs use a /64 for the loopback interface and some may have multiple LAN segments predefined (for example Guest WiFi network and wired LAN), so as soon as there is more than one LAN segment behind the CE, exceptions will have to be added to the ISP provisioning system that will greatly complicate management. It is not possible to assign less than a /64 to each LAN port/segment/subnet/VLAN due to IPv6 protocol requirements (SLAAC, ND, etc..) that reserve the last 64 bits of the IPv6 addresses for the hosts.

Recent documents such as [RFC7934], [RFC8273], [RFC9762] and [RFC9663] show that it is beccoming more convenient to assign /64 to each host interface (e.g. for security, isolation of customers, or having many virtual machines or containers on a single host), again explaining the need for delegating many /64s to each customer.

A growing number of operators are also using prefix colouring to deploy products with distinct Service Level Agreements (e.g. voice, data, video) and this requires at least a unique /64 for each product or service. If combined with home networking technologies, the number of prefixes increases quite quickly and delegation of multiple IPv6 prefixes at the same time will occur, so assignments of less than /56 will probably require renumbering in the near future.

The Broadband Forum also recommends a similar approach in their [TR-177] document: "A delegated prefix for use within the home network (mandatory). The Broadband Forum suggests a size for the delegated prefix of least a /60 for home network or SOHO environments, with a recommended prefix length of /56. The delegated prefix may be extended to a /48 for larger organizations.".

4.4. Considerations for Cellular Operators

There is a clear exception to the rules described above when assigning prefixes in a cellular network. In this case, a /64 will need to be provided for each PDP context for cellular phones, whereas for celullar modems/routers, i.e. in the case of broadband by means of cellular access, it will still be necessary to choose a /48, /52 or /56 in accordance with the aforementioned considerations.

5. Assigned Prefix Persistence Considerations

Because the scarcity of IPv4 addresses, the most common practice for service providers was to assign temporary or "dynamic" leases of addresses to the CEs. We could not actually say this was a real "best practice", but instead the only choice to share addresses among the majority of the customers, and then use exceptions in provisioning systems for "static" leases of individual addresses, avoiding manual configurations. We could also say that it is a best practice for end-site IPv4 routed prefixes to be assigned in such way that makes them permanent.

In the end, this created some wording confusion, because "dynamic" is associated to DHCP, which is "the protocol" typically being used for those leases, even if they are "static" (vs "manual" configuration). This is the reason, to avoid wording confusion, is preferable to use a differenciated terminology: persistent vs non-persistent instead of dynamic/static.

Persistent prefix assignment means that a prefix is assigned to a customer and that prefix will always remain the same regardless of how many times the customer (re)connects or renews the lease. Typically this is achieved by means of an AAA mechanism, which may be dependent on DHCPv6 and/or other provisioning systems. It is “persistent prefix” for the same customer in the same link/location regardless of the provisioning system being used.

DHCPv6-PD [RFC8415] is commonly used for non-persistent assignments, in the same way it is common for IPv4, where a bigger pool of IPv6 space is assigned to each termination point (PoP with BNG, BRAS, etc.), and so as customers connect, they are randomly assigned prefixes from this when they (re)connect or the lease time expires. They may get the same prefix, but typically it will be different (non-persistent) unless the lease time is so high that it effectively become “persistent”. In this case, a customer will get the same prefix even if they switch off their router for several days, weeks or months, depending on the lease time.

5.1. Non-persistent assignments perceived as ’easier’

When faced with the task of how to deploy IPv6, it is easy to go for an option that you’re used to (in IPv4), initially requires less effort, time and energy. However, this will usually create more problems later on. As we indicaded before, IPv6 is not the same as IPv4, and best current practices in IPv4 are not neccesarily best current practices in IPv6, most of the time in the other way around, they may somehow ruin your deployment efforts.

The easiest method is to assign prefixes from a pool of IPv6 prefixes to termination points (BNG, BRAS or other equipment, depending on the type of access network) and let the provisioning system decide what customers will get when they connect and ask for a prefix delegation over DHCPv6-PD. As already indicated above, this practice is carried over from the IPv4 world where addresses are commonly assigned "dynamically" (non-persistent) and where CEs perform NAT to conserve IPv4 space. Bear in mind that end-sites with an IPv4 subnet behind their CE never got “non-persistent” assigned IPv4 prefixes as this would require reconfiguration of all hosts on their network every few hours or days. Instead they are typically using private IPv4 addresses as per [RFC1918], which get translated by the NAT to a single public IPv4 address or a small block of them. By contrast, because there is no scarcity of IPv6 addresses, NAT is not needed and every IPv6 end-site can get a sufficiently big IPv6 prefix so it is unnecessary to apply this extra complexity of the “IPv4 model” to IPv6.

Non-persistent prefix assignment also appears initially easier as it facilitates aggregation of internal routing tables according to end customer connection termination points. Every termination point has its own pool of IPv6 prefixes that are nicely aggregable, whilst it may appear that with persistent IPv6 prefix assignments it is necessary to discover which customer is terminated at which termination point, group them into larger IPv6 pools, and then update our database accordingly. However, this is resolved by the provisioning system doing it in the other way around: from an AAA database, which is typically tied to an IPAM for the initial assignment to each new customer. In this way, when a new end-site joins a network for the first time, it is provisioned with a prefix from the pool assigned to the PoP where it actually connects (so it is already agregatted in that PoP), and this information is recorded in the AAA for future connections. Note also that in many networks, depending on their size there may be a single PoP, so this is a lesser issue.

Some operators may wonder what happens when a customer moves to another city or neighbourhood. Moving to a different location means all the equipment is switched off whilst transporting it and if services must remain on-line, clearly there has been some previous planning, services have been replicated in the new end-site, and probably there was a need to reconfigure them, including an actual renumbering with the new assigned prefix. Since it will be necessary to provision the new connection elsewhere, then it is perfectly fine to also change the prefix of the customer to match the criteria for that aggregation point. This can be avoided if the new end-site link is in the same “aggregation region/point” and the customer can be off-line for a certain period of time while moving the equipment from one location to another. If the customer specifically requests that the same IPv6 prefix moves with them across different aggregation points, service providers may need special internal routing table changes and the service provider may decide to offer that service at an extra cost or not offering it at all. However, that should be an uncommon scenario.

5.2. Non-persistent assignments considered harmful

Taking a scenario where there is a connected CE with a dynamically assigned prefix (e.g. 2001:db8:aaaa::/48). The WAN link may use the first /64 segment (2001:db8:aaaa:0::/64) and the CE may sub-assign local loopback addresses out of the first /64 segment (2001:db8:aaaa:1::/64) and sub-assign 2001:db8:aaaa:2::/64 to the first LAN interface (probably bridged with the main WiFi SSID). At the same time, there may be a guest WiFi SSID (2001:db8:aaaa:3::/64) and even a specific WiFi SSID for IoT devices (2001:db8:aaaa:4::/64). As there are some smart devices running containers of VMs in the network (even exposing services to Internet), there may be some additional /64s sub-assigned to their interfaces and moreover, some shorter prefixes, for example /60s for other parts of the network.

So, to make it simple, let’s consider that the hosts on the default/ main wired/WiFi network autoconfigure IPv6 addresses out of 2001:db8:aaaa:2::/64 segment and start communicating with the rest of the Internet.

Now all of a sudden there is a power outage (which is very common in many regions/countries in the world, even “highly-developed” countries) or the CE freezes and reboots and the connection has to be established again. This time a new IPv6 prefix is assigned: 2001:db8:bbbb::/48. If the CE knows that the delegated prefix has changed, it should send out RA packets with a prefix valid lifetime of 0 to tell all devices that the old addresses are no longer valid. However, the CE rarely knows that before the reboot there was a different prefix on the network, and the packets to revoke the old

IPv6 addresses do not get sent. In this case, multiple IPv6 addresses from completely different assigned prefixes end up on the same network interface, some of which will no longer work and may imply increase the number of claims to the service provide help desk. This gets even more complicated if there are multiple consecutive power outages (very common as well) affecting the CE.

Just consider the added complexity of the other prefixes being sub-assigned across the different segments on the network, either using SLAAC or DHCPv6-PD. All them keep trying connecting to Internet using the old prefix.

Different OS vendors treat this scenario differently, but there often ends up being a wrong source IPv6 address for sending packets through the CE out to the Internet. As the network operator’s equipment deleted the previous delegated prefix route back to the CE, any return packets never reach the originating device and IPv6 connectivity will be broken until the old IPv6 addresses time-out and are automatically removed from the interfaces. If another reconnection to the ISP is required in the interim, there will be a third set of IPv6 addresses from yet another assigned prefix, and this will cause even more confusion.

Several big content providers and device vendors are measuring “IPv6 brokenness” in operator networks by matching the SYN, SYN ACK and ACK packets received/sent to/from a single source. If they see a SYN and send back SYN ACK, but never receive ACK in a timely manner, they slowly stop serving AAAA records for the ASNs where they see this, as they prefer a stable IPv4 connectivity even if it presents a higher latency (due to NATs/CGNs), versus a bad IPv6 network. It is a matter of those services or device vendors offering "best quality of service" to their customers. So, assigning IPv6 non-persistent prefixes, can imply that some content providers or device vendors start ignoring your IPv6 traffic quite quickly and force your customers back to IPv4. And these are usually destinations (big content providers) where you will be sending a significant amount of traffic. Clearly this has implications in networks using CGN, as the usage of CGN will significantly increase.

Using non-persistent prefixes also means that it is necessary to have a logging system that registers which WAN and LAN prefixes are being used at each moment by each customer site, which additional storage capacity, in order to comply with legal/regulatory requirements.

Finally, if users have services exposed to Internet, such as web, email or VPNs, they typically need to manually configure the addresses of those, so using non-persistent prefixes is not an option in this case. With the growth of broadband capacities (such as

FTTH), it is becoming more and more common that end-sites run servers or services on their LANs, including the likes of IP cameras or security systems in a home. Persistent prefixes allows FQDNs to be assigned to individual addresses of those prefixes. In fact, persistent-prefixes offers the service providers the oportunity to sell/resell value added services to customers, including managed DNS services, without the complexity of developing systems that continuously keep track of the prefixes assigned to each customer.

Using non-persistent prefix delegation, enforces the service providers to verify that the CEs used by the customers will not have the problems described above. Commonly this can not be ensured, so the current best practice is to avoid using non-persistent prefixes.

It also needs to be realised that non-persistent prefixes have other implications and additional OPEX, because it is not only the CEs that need to be numbered, but all the devices behind them in the customer LANs as well. Different implementations can have very different behaviors that may affect the number of support calls to service provider help-desk every time a prefix changes.

Last, but not least, exactly the same as with IPv4, when the end-site IPv6 assigned prefix is renumbered, even if correctly done by the service provider (instead of a power outage or CE reboot), many running applications will not survive, creating problems to users and applications, which in turn can imply subsequent help-desk calls and even possible legal or consumer claims.

This has been extensively described in [RFC8978] and a solution proposed by [RFC9096]. The standard updates required for a definitive solution is work in progress in [I-D.ietf-6man-slaac-renum]. Note that even when this document is approved, it doesn’t resolve many issues, such as those related to manual configuration changes required in the network, for instance, DNS, devices renumbering, servers, containers or VM renumbering. In addition to that, it may take many years to get implemented in CEs and we know that many of them remain operating in the networks without firmware updates for many years, so is not a practical solucion to "wait".

5.3. Persistent assignments are the best current practice

As already mentioned, a best practice in IPv4 was to assign persistent IPv4 prefixes whilst giving an end-user a routed prefix, and same is true for IPv6 where persistent prefix assignment is strongly recommended. It is comparable to assign IPv4 prefixes to assigning IPv6 ones. It is not comparable to assign IPv4 addresses to IPv6 prefixes.

If required for provisioning, the connection between a network and the end-site CE can be non-persistent using /64 (or even /127 if the equipment supports it), but choosing persistent IPv6 assigned prefixes for end-user LANs will avoid a lot of difficulties experienced by some earlier IPv6 network operators.

This is especially the case where there are non-residential customers as well, which typically will use residential links, as this means you can have a single provisioning system and it is unnecessary to maintain a logging system, increasing also the security of the network because the undubitable identificacion of end-sites and disallowing connections for end-sites that have not the proper authorization in the AAA. This is because each end-site always have the same prefix(es) and can be identified in the AAA or provisioning system, reducing complexity and making things cheaper. A bit of initial thought, planning and consideration for future needs can therefore save a great deal of time and energy when IPv6 has been deployed.

From the economic/business perspective, another important consideration with persistent prefixes is that it is possible to ‘name’ value added services using DNS (e.g. camera1.username.ispname.com) that can result in considerable new income streams. Trying to deploy new services or applications with non-persistent prefixes is always more difficult and costly, and will increase time spent on operations, management and troubleshooting. This is just one example to make clear that persistent prefixes enable innovation, new services and applications, which in turn means new business possibilities.

Further to the above, it should be noted that persistent assignments of prefixes to customers may increase the incentive for customers to remain with that ISP, and result in decreased customer churn.

Finally, if the use of persistent prefixes is not feasible for unavoidable technical reasons, using non-persistent but long-lived assignments must be considered, so the lease time is as long as the provisioning system allows. Note that there are several choices to keep end-sites correctly correlated to the AAA information for the correct prefix provisioning, and not just differentiated user/password (which in many service providers is the same for all the customers to simplify the CE provisioning). For example, using UUIDs or DUIDs [RFC6355]/[RFC8415]. Even in the case where DHCPv6 relay are required, Relay Agent Remote-ID (37) can be used as per [RFC4649].

It should be remarked that persistence of prefixes shoud be expected only when customers are connected to the same aggregation point. Outside of that, customers moving to different locations, has different routing and consequently business considerations.

6. Best Common Practices Summary for IPv6 Prefix Assignments

We can summarize the best common practices for IPv6 prefix assignments to end-sites as follows:

1. The prefix assigned to end-site MUST be a GUA /48, using DHCPv6-PD [RFC8415].

2. The prefix assigned to end-site MUST be persistent.

3. The prefix for the WAN link point-to-point SHALL be a GUA /64. A /127 MAY be used for the actual numbering of the interfaces in each side.

4. It is RECOMMENDED that the prefix for the WAN point-to-point is the first /64 from the assigned end-site prefix, using the Prefix Exclude Option for DHCPv6-based Prefix Delegation ([RFC6603]).

5. The assigned prefix MUST NOT, ever, be longer than /56.

7. Security Considerations

This document does not have any new specific security considerations.

8. IANA Considerations

This document does not have any new specific IANA considerations.

9. Acknowledgements

The author would like to acknowledge the inputs of Mikael Abrahamsson, Brian Carpenter, Eric Vyncke and Mark Smith on previous versions of this work.

Acknowledge is also due to my co-authors of RIPE-690 ("Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose", https://www.ripe.net/publications/docs/ripe-690) and global community, which provided valuable inputs that were key for this document.

Acknowledgement to co-authors, Cesar Olvera and Miguel Angel Daz, of a previous related document (draft-palet-v6ops-point2point, 2006), as well as inputs for that version from Alain Durand, Chip Popoviciu, Daniel Roesen, Fred Baker, Gert Doering, Olaf Bonness, Ole Troan, Pekka Savola and Vincent Jardin, are also granted.

10. References

10.1. Normative References

[I-D.ietf-6man-slaac-renum]
Gont, F., Zorz, J., Patterson, R., and J. Linkova, "Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events", Work in Progress, Internet-Draft, draft-ietf-6man-slaac-renum-10, 3 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-slaac-renum-10>.

[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>.

[RFC3769] Miyakawa, S. and R. Droms, "Requirements for IPv6 Prefix Delegation", RFC 3769, DOI 10.17487/RFC3769, June 2004, <https://www.rfc-editor.org/info/rfc3769>.

[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>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, DOI 10.17487/RFC4649, August 2006, <https://www.rfc-editor.org/info/rfc4649>.

[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>.

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, DOI 10.17487/RFC6355, August 2011, <https://www.rfc-editor.org/info/rfc6355>.

[RFC6603] Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, DOI 10.17487/RFC6603, May 2012, <https://www.rfc-editor.org/info/rfc6603>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

[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>.

[RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi, "Host Address Availability Recommendations", BCP 204, RFC 7934, DOI 10.17487/RFC7934, July 2016, <https://www.rfc-editor.org/info/rfc7934>.

[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>.

[RFC8273] Brzozowski, J. and G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273, DOI 10.17487/RFC8273, December 2017, <https://www.rfc-editor.org/info/rfc8273>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC9096] Gont, F., or, J., Patterson, R., and B. Volz, "Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events", BCP 234, RFC 9096, DOI 10.17487/RFC9096, August 2021, <https://www.rfc-editor.org/info/rfc9096>.

[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>.

[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>.

[RFC9818] Winters, T., "DHCPv6 Prefix Delegation on IPv6 Customer Edge (CE) Routers in LANs", RFC 9818, DOI 10.17487/RFC9818, July 2025, <https://www.rfc-editor.org/info/rfc9818>.

10.2. Informative References

[IPv6-Survey] Palet Martinez, J., "IPv6 Deployment Survey (Residential/ Household Services)", January 2018, <https://indico.uknof.org.uk/event/41/contribution/5/material/slides/0.pdf>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC3627] Savola, P., "Use of /127 Prefix Length Between Routers Considered Harmful", RFC 3627, DOI 10.17487/RFC3627, September 2003, <https://www.rfc-editor.org/info/rfc3627>.

[RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", RFC 6164, DOI 10.17487/RFC6164, April 2011, <https://www.rfc-editor.org/info/rfc6164>.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <https://www.rfc-editor.org/info/rfc6583>.

[RFC6752] Kirkham, A., "Issues with Private IP Addressing in the Internet", RFC 6752, DOI 10.17487/RFC6752, September 2012, <https://www.rfc-editor.org/info/rfc6752>.

[RFC7404] Behringer, M. and E. Vyncke, "Using Only Link-Local Addressing inside an IPv6 Network", RFC 7404, DOI 10.17487/RFC7404, November 2014, <https://www.rfc-editor.org/info/rfc7404>.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015, <https://www.rfc-editor.org/info/rfc7608>.

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016, <https://www.rfc-editor.org/info/rfc7707>.

[RFC8978] Gont, F., or, J., and R. Patterson, "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events", RFC 8978, DOI 10.17487/RFC8978, March 2021, <https://www.rfc-editor.org/info/rfc8978>.

[RIPE-690] "Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose", October 2017, <https://www.ripe.net/publications/docs/ripe-690/>.

[TR-177] The Broadband Forum, "TR-177 - IPv6 in the context of TR-101", November 2017, <https://www.broadband-forum.org/pdfs/tr-177-1-0-1.pdf>.

Author’s Address

Jordi Palet Martinez
The IPv6 Company
Molino de la Navata, 75
28420 La Navata - Galapagar Madrid
Spain
Email: jordi.palet@theipv6company.com
URI: http://www.theipv6company.com/