

IPv6 无状态地址自动配置 (SLAAC)

“ 网络上的每个 IPv6 节点都需要一个全球唯一的地址来在其本地网段之外进行通信。但是节点从哪里得到这样的地址呢？有几个选项：

网络上的每个 IPv6 节点都需要一个全球唯一的地址来在其本地网段之外进行通信。但是节点从哪里得到这样的地址呢？有几个选项：

- 手动分配 - 每个节点都可以由管理员手动配置 IPv6 地址。它不是一种可扩展的方法，并且容易出现人为错误。
- DHCPv6 (动态主机配置协议第 6 版) - 最广泛采用的用于为主机动态分配地址的协议。需要网络上的 DHCP 服务器和其他配置。
- SLAAC (无状态地址自动配置) —— 它被设计成一种更简单、更直接的 IPv6 自动寻址方法。在 RFC 4862 中定义的当前实现中，SLAAC 不向主机提供 DNS 服务器地址，这就是它目前未被广泛采用的原因。

在本课中，我们将了解 SLAAC 的工作原理以及与 DHCPv6 相比使用它的优缺点。

什么是 SLAAC？

SLAAC 代表无状态地址自动配置，这个名字几乎解释了它的作用。它是一种机制，使网络上的每个主机都能够自动配置唯一的 IPv6 地址，而无需任何设备跟踪哪个地址分配给哪个节点。



在地址分配的上下文中，无状态和有状态的含义如下：

- 有状态地址分配涉及跟踪每个分配状态的服务器或其他设备。它跟踪地址池的可用性并解决重复的地址冲突。它还记录每个分配并跟踪到期时间。
- 无状态地址分配意味着 没有服务器跟踪已分配的地址以及仍可用于分配的地址。同样在无状态分配场景中，节点负责按照以下逻辑解决任何重复的地址冲突：生成 IPv6 地址，运行重复地址检测 (DAD)，如果该地址恰好在使用中，则生成另一个地址并再次运行 DAD，ETC。

SLAAC 是如何工作的？

为了充分了解 IPv6 自动寻址的工作原理，让我们按照 IPv6 节点从连接到网络的那一刻到它拥有唯一的全球单播地址的那一刻所采取的步骤进行操作。

第 1 步：节点为自己配置一个链路本地地址

当 IPv6 节点连接到启用 IPv6 的网络时，它通常做的第一件事是使用本地链路地址自动配置自身。此本地地址的目的是使节点能够在第 3 层与本地网段中的其他 IPv6 设备进行通信。最广泛采用的自动配置链路本地地址的方法是结合链路本地前缀 FE80::/64 和 EUI-64 接口标识符，从接口的 MAC 地址生成。

图 1 显示了如何从 MAC 地址 7007.1234.5678 生成本地地址的分步示例。



1. Take the interface's MAC address (for this example 7007.1234.5678):

70	07	12	34	56	78
----	----	----	----	----	----

2. Insert 0xFFFE in the middle of the MAC address:

70	07	12	FF	FE	34	56	78
----	----	----	----	----	----	----	----

3. Flip the 7th bit of the MAC address. (Note that the MAC is written in HEX, to flip the 7th bit we must convert the first two HEX digits to BINARY):

70	07	12	FF	FE	34	56	78
----	----	----	----	----	----	----	----

To binary

01110000

Flip the 7th bit

01110010

To HEX

72	07	12	FF	FE	34	56	78
----	----	----	----	----	----	----	----

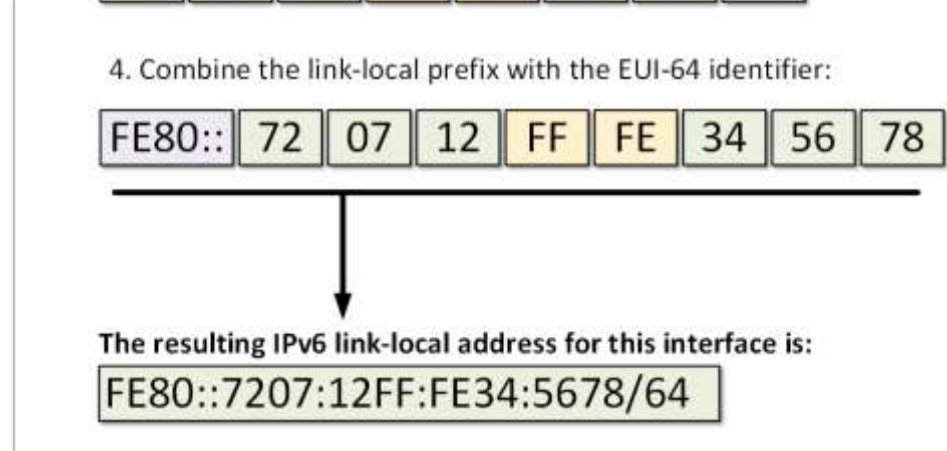


图 1. 从接口的 MAC 地址生成链路本地地址

完成上述步骤后，节点就有了一个功能齐全的 EUI-64 格式的链路本地地址，如下所示：

```
C:\>ipconfig /all
```

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix.:

Physical Address.....: 7007.1234.5678

Link-local IPv6 Address.....: FE80::7207:12FF:FE34:5678

IP Address.....: 0.0.0.0

Subnet Mask.....: 0.0.0.0

Default Gateway.....: 0.0.0.0

DNS Servers.....: 0.0.0.0

DHCP Servers.....: 0.0.0.0

DHCPv6 Client DUID.....: 00-01-00-01-C4-35-08-8E-70-07-12-34-56-78

第 2 步：节点执行重复地址检测 (DAD)

在 IPv6 主机自动配置其本地链路地址后，它必须确保该地址在本地网段中实际上是唯一的。即使另一个节点具有相同的确切地址的可能性非常小。它必须执行称为重复地址检测 (DAD) 的过程。

DAD 是一种涉及称为请求节点多播的特殊类型地址的机制。配置 IPv6 地址后，每个节点都会加入一个由地址 FF02::1:FFxx:xxxx 标识的多播组，其中 xx:xxxx 是 IPv6 单播地址中的最后 6 个十六进制值。因此，对于每个已配置的单播地址，无论是本地链路还是全局地址，主机都会加入相应的自动生成的请求节点多播组。

在我们的示例中，链路本地地址的最后 6 个十六进制值是 34:5678，因此节点加入了多播组 FF02::1:FF 34:5678。由于 PC1 运行的是 Windows 10 操作系统，我们可以使用以下命令进行验证：

```
C:\>netsh interface ipv6 show joins
```

Interface 8: Ethernet0

Scope	References	Last	Address
-------	------------	------	---------

0	0 Yes	ff01::1
---	-------	---------

0	0 Yes	ff02::1
---	-------	---------

0 1 Yes ff02::c

0 2 Yes ff02::fb

0 1 Yes ff02::1:3

0 2 Yes ff02::1:ff34:5678

考虑到这个逻辑，我们知道如果另一台主机具有相同的确切链接本地地址，它还将侦听从该地址自动生成的请求节点多播组上的消息 - FF02::1:FF34:5678 . 为了让 PC1 进行检查，它发送一个 ICMPv6 消息，其中目标地址设置为该组，源地址设置为 IPv6 未指定地址。在数据包的 ICMPv6 部分中，PC1 将整个地址放在目标地址字段中。图 2 说明了该过程。然后 PC1 在网络上发送数据包。只有正在监听这个确切的自动生成的多播组的节点才会打开数据包，所有其他节点都会丢弃它。如果任何节点的 IPv6 地址具有相同的最后 6 个十六进制数字，则将查看 ICMPv6 部分并检查目标地址是否与它自己的任何地址匹配。如果匹配，主机将回复此 IPv6 地址已在使用中。如果没有人回复，PC1 将断定此地址是唯一的并且可以使用，并将分配它。

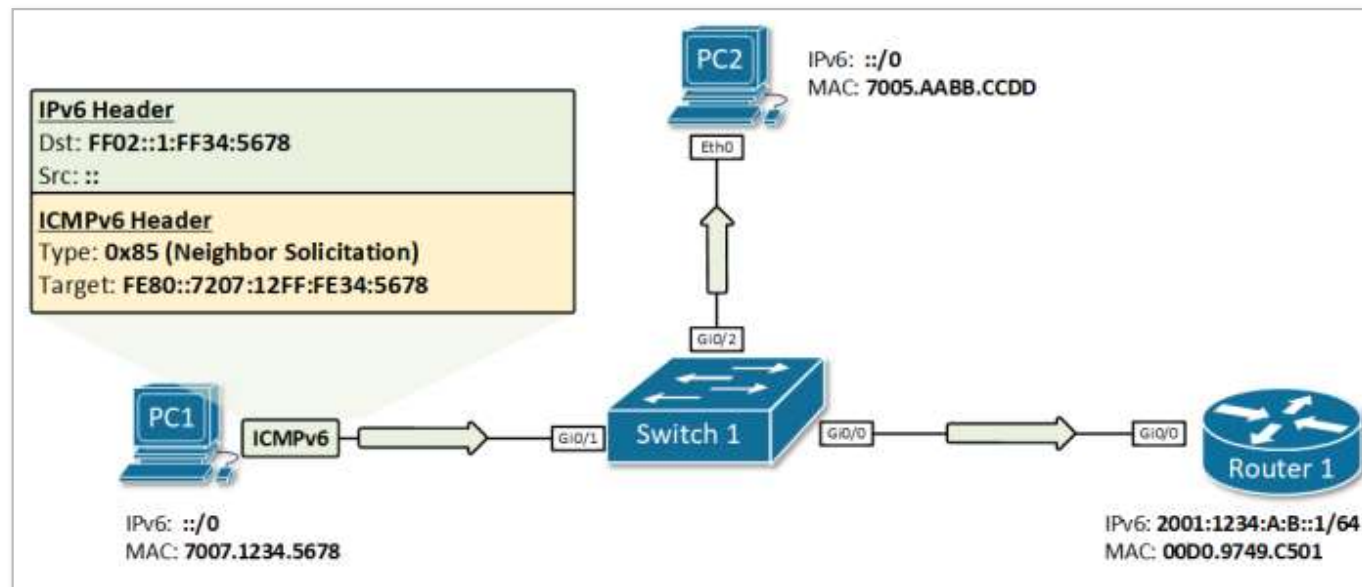


图 2. PC1 对其本地链路地址执行 IPv6 DAD

此过程称为重复地址检测 (DAD)，并在每次分配新地址时完成。在我们的示例中，PC1 发送 ICMPv6 Neighbor Solicitation 消息，如图 2 所示，没有人回复。然后，PC1 将确定该链接本地地址在该本地段中是唯一的。

第 3 步：节点发送 Router Solicitation 消息

此示例中的步骤 1 和 2 描述了生成和分配唯一链接本地地址的过程。此过程不完全是无状态自动配置功能的一部分，但如果没有链路本地地址，PC1 将无法在第 3 层与任何其他 IPv6 节点进行通信。因此，这是 SLAAC 工作的先决条件，这就是我们将其包含在示例中的原因。

在 PC1 拥有链路本地地址后，它现在可以开始使用 SLAAC 自动配置全局单播地址的过程。此过程的第一步是发送称为路由器请求 (RS) 的 ICMPv6 消息。该消息的目的是“询问”连接到该网段的所有 IPv6 路由器所使用的全局单播前缀。目标地址是所有路由器的多播地址 FF02::2，对于源，PC1 使用其链路本地地址。请注意，只有路由器订阅了多播组 FF02::2，这意味着只有路由器 1 会处理此消息，本地网段上的所有其他节点都会丢弃它。

在路由器 1 收到路由器请求消息后，它会返回一个称为路由器广告 (RA) 的 ICMPv6 消息。RA 消息包括链路上的全局 IPv6 前缀和前缀长度。在我们的示例中，这些将是前缀 2001:1234:A:b:: 和 /64 的前缀长度。对于这个 RA 数据包的源，路由器 1 使用自己的链路本地地址，目标是所有节点的多播地址 FF02::1。该过程如图 3 所示。



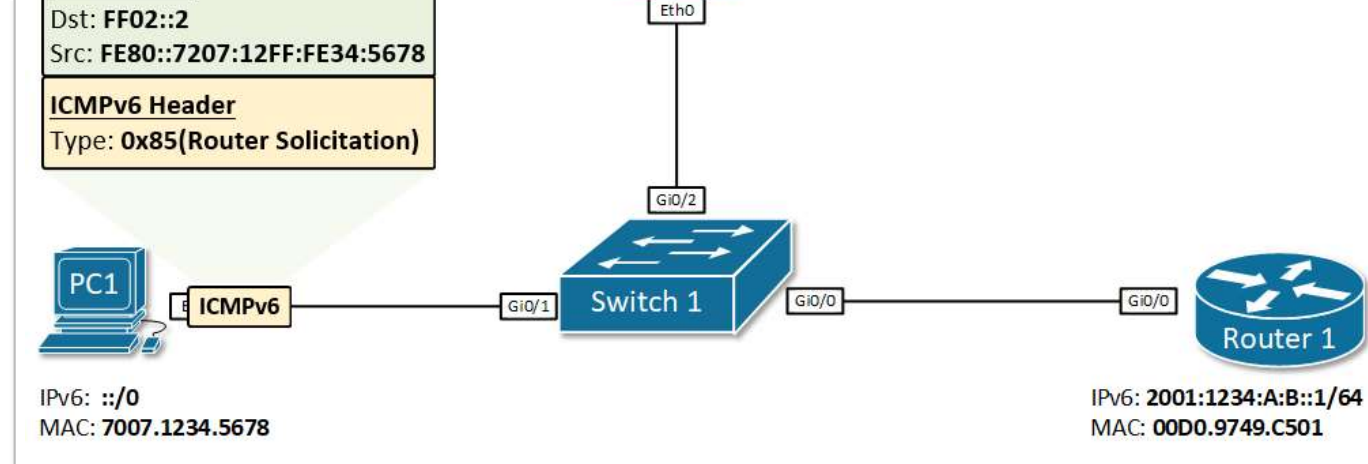


图 3. IPv6 无状态地址自动配置示例

第 4 步：节点配置其全局单播地址

一旦 PC1 从路由器 1 取回路由器通告，它将前缀 2001:1234:A:B::/64 与其 EUI-64 接口标识符 (7207:12FF:FE34:5678) 组合在一起，从而产生全球单播地址 2001:1234:A:B:7207:12FF:FE34:5678/64。因为路由器通告来自路由器 1，所以 PC1 将其 IPv6 默认网关设置为 R1 的链路本地地址。

现在 PC1 有一个全球单播地址和一个默认网关。但 SLAAC 过程并未完成。PC1 必须确定这个自动生成的地址在本地网段中是唯一的。因此，PC1 执行重复地址检测 (DAD) 过程。

第 5 步：节点执行重复地址检测 (DAD)

我们已经在步骤 2 中详细解释了 DAD 过程。当 PC1 自动生成其全局单播地址时，它立即加入自动生成的请求节点组播组 FF02::1:FF34:5678。为了确保没有其他人在使用这个地址，PC1 然后向请求节点地址 FF02::1:FF34:5678 发送一个名为 Neighbor Solicitation 的 ICMPv6 消息，

并等待节点是否回复。如果没有收到回复，PC1 知道该地址是唯一的，并且可以开始使用它进行本地网段之外的通信，包括在 Internet 上的通信。

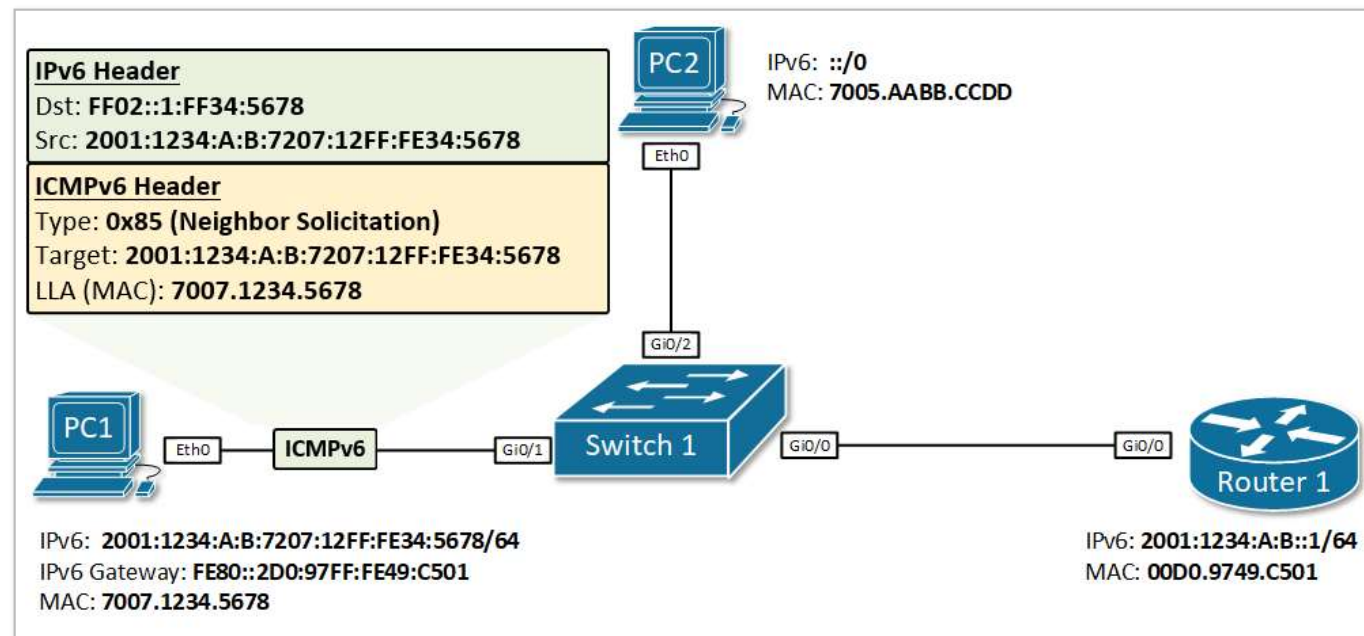


图 4. IPv6 重复地址检测

SLAAC 的问题

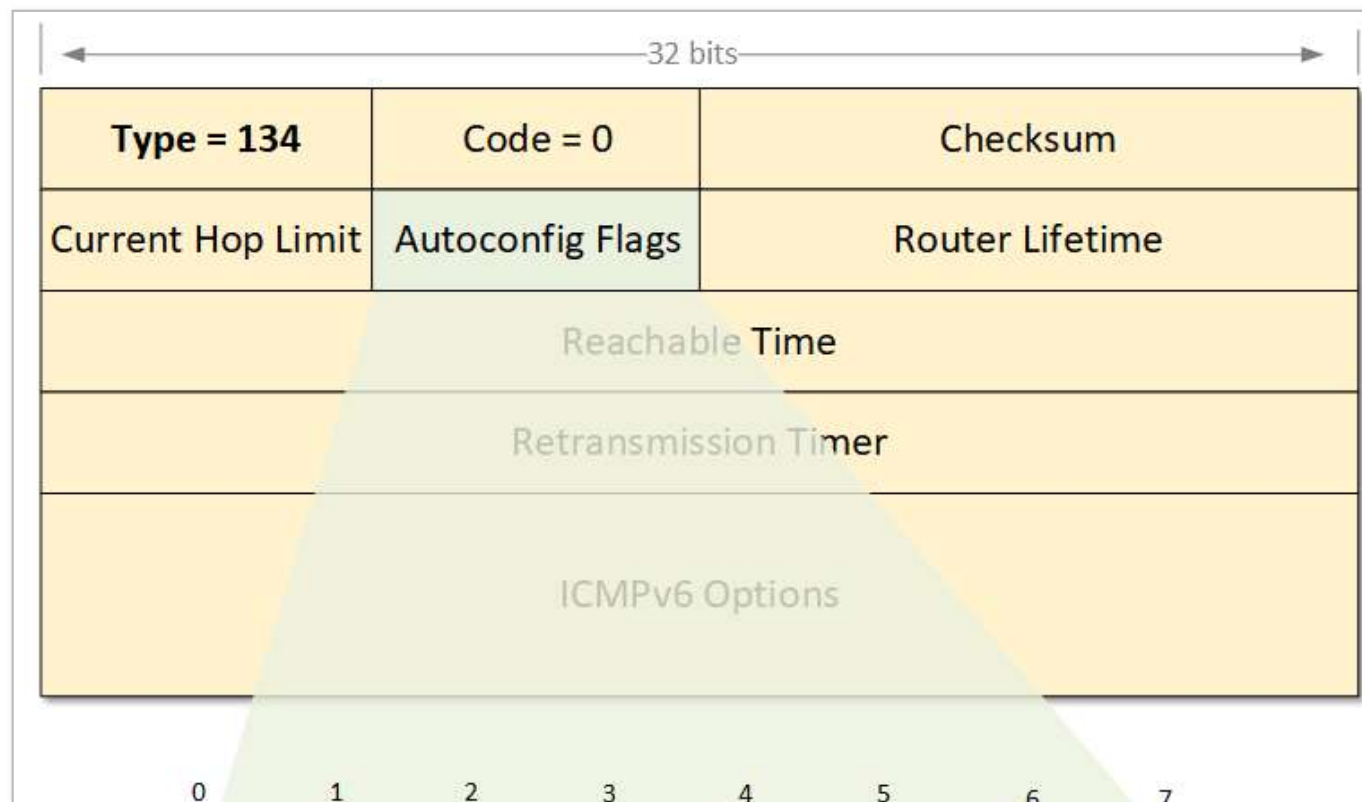
到现在为止还挺好。我们已经看到节点如何自动配置全球唯一的 IPv6 地址和默认网关。

但是，SLAAC 不提供 DNS 信息，没有 DNS，很多服务如上网是不可能的。

Router Advertisement 标头中有一个字段，旨在解决此问题。

路由器通告标志

正如我们上面所说，默认情况下，SLAAC 不提供 DNS。如果没有 DNS，许多需要从 URL 地址解析到 IP 的服务将无法运行。RA 消息中有一个字段可帮助节点了解从何处获取 IPv6 地址和 DNS 信息。



M flag	O flag		Prf flag	Reserved	

图 5. 检查路由器通告标志

如果 M-flag 设置为 1，则表明地址可通过 DHCPv6 获得。路由器基本上是在告诉节点向 DHCP 服务器询问地址和 DNS 信息。如果设置了 M 标志，则可以忽略 O 标志，因为 DHCPv6 将返回所有可用信息。

如果 O-flag 设置为 1，则表明 DNS 信息可通过 DHCPv6 获得。路由器基本上是告诉节点通过 SLAAC 自动配置地址并向 DHCP 服务器询问 DNS 信息。

如果既没有设置 M 也没有设置 O 标志，这表明网段上没有可用的 DHCPv6 服务器。

Prf 标志（默认路由器首选项）可以设置为低 (1)、中 (0) 或高 (3)。当一个节点从多个路由器接收到路由器通告消息时，默认路由器首选项 (DRP) 用于确定首选哪个路由器作为默认网关。

The image shows a Wireshark packet capture of an ICMPv6 Router Advertisement (Type 134). The packet details pane shows the following fields:

- Type: Router Advertisement (134)
- Code: 0
- Checksum: 0x3d3e [correct]
- Cur hop limit: 64
- Flags: 0x00, Prf (Default Router Preference): Medium
- Router lifetime (s): 1800
- Reachable time (ms): 0
- Retrans timer (ms): 0
- ICMPv6 Option (Source link-layer address : 50:00:00:01:00:00)
- ICMPv6 Option (MTU : 1500)
- ICMPv6 Option (Prefix information : 2001:1234:a:b::/64)

Three callouts provide additional context:

- Green callout:** When set, it indicates that addresses are available via DHCPv6. If the M flag is set, the O flag is redundant and can be ignored.
- Blue callout:** When set, it indicates that other configuration information (typically DNS-related) is available via DHCPv6.
- Yellow callout:** When a node receives RA messages from multiple routers, the Default Router Preference (DRP) is used to determine which router to prefer as a default gateway.

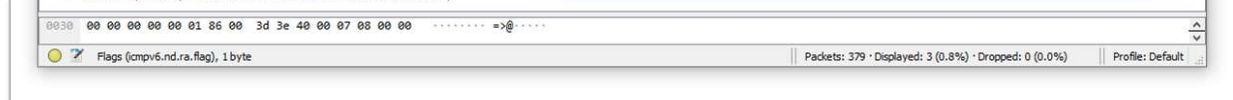


图 6. 使用 Wireshark 检查路由器通告标志

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎^{beta}，[点击查看详细说明](#)

