

通 信 标 准 类 技 术 报 告

YDB 041—2009

IPv6 协议密码生成地址安全扩展 技术要求

Cryptographically generated addresses extension in IPv6

2010-01-14 印发

中国通信标准化协会

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 IPv6 Internet protocol version 6	1
3.2 IPv6 地址	1
3.3 IPv6 基本头	1
3.4 IPv6 地址扩展头	1
3.5 CGA cryptographically generated addresses.	1
3.6 CGA 参数	2
3.7 节点	2
3.8 TLV 选项	2
4 CGA 原理概述	2
5 密码生成地址扩展头在 IPv6 扩展头中的顺序	2
6 密码生成地址扩展头格式	3
6.1 密码生成地址请求扩展头格式	3
6.2 密码生成地址参数扩展头格式	4
6.3 密码生成地址签名扩展头格式	4
7 数据包处理规则	4
7.1 数据包发送处理规则	5
7.2 数据包接收处理规则	5
8 ICMP 消息	5
8.1 验证失败	5
8.2 缺少必要选项	6
9 密码生成地址扩展头应用举例	6
10 密码生成地址的产生和配置	7
10.1 密码生成地址的参数格式	7
10.2 参数和地址的生成	8
10.3 配置节点的密码生成地址	8

前 言

密码生成地址扩展作为 IPv6 的一个新增扩展头，利用密码生成地址和公钥绑定的特点，无需其它任何第三方或安全基础设施，可以提供源地址验证和信息完整性验证等，对 IPv6 网络安全性能提高有重要意义，为此制定本技术报告。

为适应信息通信业发展对通信标准文件的需要，在信息产业部统一安排下，对于技术尚在发展中，又需要有相应的标准性文件引导其发展的领域，由中国通信标准协会组织制定“通信标准类技术报告”，推荐有关方面参考采用。有关对本技术报告的建议和意见，向中国通信标准化协会反映。

本技术报告由中国通信标准协会提出并归口。

本技术报告起草单位：华为技术有限公司。

本技术报告主要起草人：冯鸿雁。

IPv6 协议密码生成地址安全扩展

技术要求

1 范围

本技术报告规定了密码生成地址在 IPv6 协议中的安全扩展，对其的处理规则，以及它在源地址验证技术方面的应用。

本技术报告适用于采用IPv6地址的网络设备。

2 规范性引用文件

下列文件中的条款通过本技术报告的引用而成为本技术报告的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术报告，然而，鼓励根据本技术报告达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本技术报告。

IETF RFC 2460	IPv6 规范
IETF RFC 3971	安全邻居发现（SEND）
IETF RFC 3972	密码生成地址（CGA）
IETF RFC 4443	适合 IPv6 规范的 ICMP (ICMPv6)

3 术语和定义

下列术语和定义适用于本技术报告。

3.1

IPv6 Internet protocol version 6
因特网协议版本6。

3.2

IPv6 地址
IPv6地址由128比特组成，包括高64比特的网络前缀和低64比特的接口标识符。

3.3

IPv6 基本头
区别于IPv4头，IPv6基本头为固定的40字节，包括4比特的版本号、8比特通信量类、20比特流标号、16比特有效载荷长度、8比特下一个首部、8比特跳数限制、128比特源地址和128比特目的地址。基本头部后面是有效载荷，它包括可能选用的扩展头和上层数据。

3.4

IPv6 地址扩展头
IPv6基本头后面允许有零个或多个扩展头，IETF RFC 2460中定义了6种扩展头，包括逐跳选项头、路由头、分片头、验证头、封装安全有效载荷头和目的站选项头。

3.5

CGA cryptographically generated addresses
密码生成地址，一种将公钥与IPv6地址绑定的方法，在IETF RFC 3972中定义。CGA基于CGA参数，生成密码的IPv6地址的接口标识符。其过程是，高64比特的网络前缀由所在子网分配，后64比特

YDB 041—2009

的接口标识符，由节点生成公私钥对，对由公钥和其他一些参数组成的CGA参数计算一个单向哈希函数，产生后64位的接口标识符。

3.6

CGA 参数

一种数据结构，在IETF RFC 3972中定义，包括修正符、网络前缀、冲突计数、公钥、扩展字段等。

3.7

节点

能够产生和识别CGA头的设备。IPv4节点或IPv6节点仅用在有必要避免混淆地方。

3.8

TLV 选项

type-length-value选项。根据选项的类型、长度、值(即选项内容)来编码的选项，见IETF RFC 2460。

4 CGA 原理概述

密码生成地址（CGA: Cryptographically Generated Addresses）是IETF RFC 3972提出来的一种无状态地址自动配置方法，如图1所示，其主要方法是：

IPv6节点首先产生公私钥对，然后用哈希算法对包含有公钥的CGA参数进行计算，得到IPv6地址的接口标识符，结合通过路由广播得到的网络前缀，得到IPv6地址，相应的私钥可以用来对从此地址发出的消息进行签名。

接收方通过重新计算的哈希值与接口标识符的比较，可以验证公钥和地址的联系。这样通过附带一个公钥，一些辅助参数及用对应于这一公钥的私钥对消息的签名，可以保护从一个IPv6地址发送来的消息。保护工作不需要认证或是任何的安全基础设施。

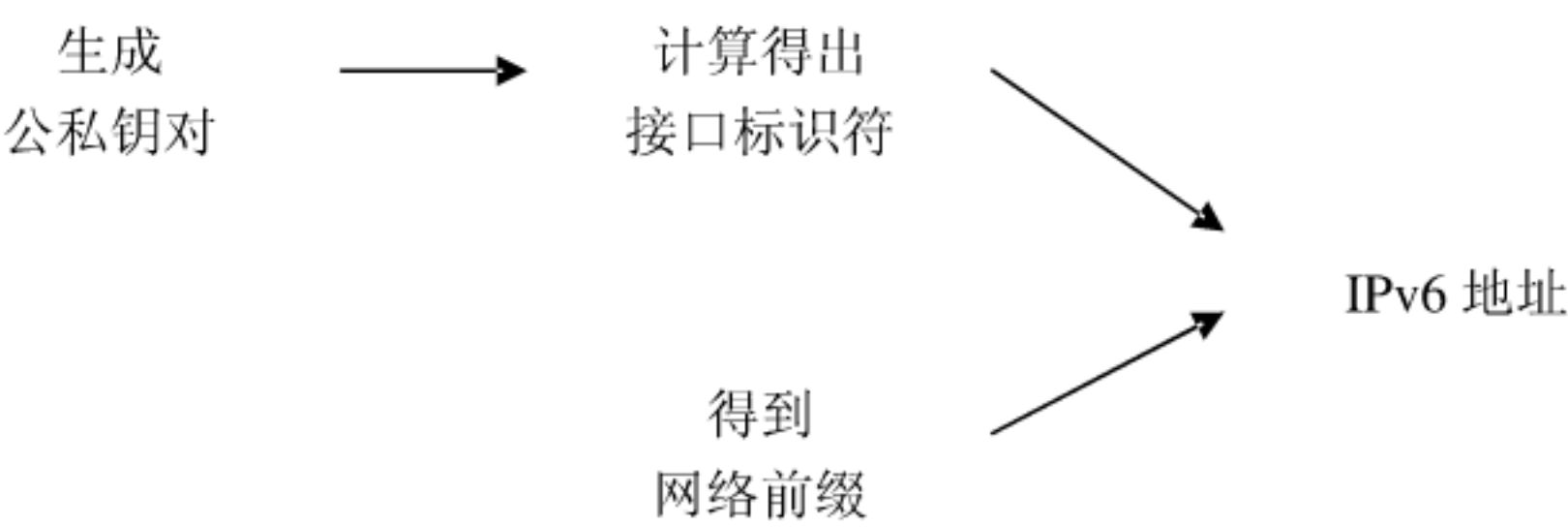


图1 密码生成地址过程

本技术报告规定了密码生成地址的扩展格式，即新定义了一个扩展头，其中包括三个可选项：CGA请求、CGA参数和CGA签名。CGA扩展头通过对对方地址和签名的验证，来确定信息来源的真实性和信息完整性。另外，由于CGA扩展头工作于网络层，网络层以上的协议都可以选择使用CGA扩展头来保护通信。

验证者需要知道被验证的地址、公钥和辅助参数值。验证完这一地址和公钥的关联性之后才能验证公钥拥有者（地址拥有者）签名的消息。但是CGA最大的优点就是不需要额外的安全基础，如公钥基础设施（PKI），权限认证或者其它值得信赖的服务器。

由于CGA自身不能被验证，虽然攻击者可以用任何子网前缀加上他自己（或其他人）的公钥，生成一个新的CGA。但攻击者不能使用其他人的CGA，也不能发送来自地址拥有者的签名消息。

5 密码生成地址扩展头在 IPv6 扩展头中的顺序

根据 IETF RFC 2460 的规定，IPv6 扩展头的顺序根据其类型，按照处理顺序安排。在所有的扩展

头中，需要网络设备处理的在数据包头的前部，需要终端处理的在数据包头的尾部。增加了 CGA 头后排列顺序如表 1（其中的数字相当于 IPv4 的协议字段的值）。

如果CGA选项的出现位置违背了上述顺序要求，IPv6节点也必须能够识别并且处理该CGA选项。

表1 CGA 头位置

IPv6 基本头
逐跳选项头
路由头
分片头
CGA 头
验证头
封装安全载荷头
目的站选项头
上层头（例如 TCP 头、UDP 头等）

6 密码生成地址扩展头格式

CGA头用于携带CGA参数等选项。CGA头的上一个头的“下一个头”字段中的值为TBD1。CGA头具体格式如下所示：

下一个头	扩展头长度	保留
选项		

- 下一个头8比特选择符，标识该选项头的下一个头类型。
- 扩展头长度8比特无符号整数，表示CGA头的长度（不包括前8字节），以字节为单位。该字段值为0时，表示CGA头中没有携带任何选项，即空CGA头。当通信一方想要使用CGA保护通信时，可以发出空CGA头；当通信一方收到空CGA头时，则向对方发出包含CGA请求选项的CGA头。
- 保留16比特字段，留待将来使用。发送时该字段必须置为0，且接收方必须忽略该字段。
- 选项该部分长度可变，可以包含零个或多个TLV选项。

本技术报告规定了 3 种选项类型，分别是 CGA 请求、CGA 参数和 CGA 签名。

- 1) CGA 请求用于请求通信对方提供 CGA 参数和 CGA 签名；
- 2) CGA 参数用于传输 CGA 参数；
- 3) CGA 签名是使用 CGA 节点的私钥对数据包负载部分的签名。

CGA头中如果包含了CGA 参数选项，则必须同时包含CGA 签名选项，否则接收方向发送方发送ICMP 错误消息至源地址；但是如果在某次通信中CGA参数已经发送过，可以仅发送CGA 签名选项，而不必同时发送CGA 参数选项。另外，对CGA头的处理方式（验证或者忽略）由接收方决定。

6.1 密码生成地址请求扩展头格式

在通信过程中，通信任意一方均可以通过发送包含了CGA 请求选项的CGA头来向对方请求CGA 参数；若接受请求，则数据包的接收方需要在响应的数据包中包含CGA 参数和CGA 签名。CGA 请求的数据格式如下：

0	8	16	24	31
类型	保留			
序列号				

YDB 041—2009

- 类型

8 比特无符号整数，值为 TBD2，表示该选项为 CGA 请求。
- 保留

8 比特字段，留待将来使用。发送时该字段必须置为 0，且接收者必须忽略该字段。
- 序列号

32 比特随机数，用于防止重放攻击。

6.2 密码生成地址参数扩展头格式

该选项用于承载 CGA 参数，接收者根据 CGA 参数对地址进行验证。CGA 参数的数据格式如下：

	0	8	16	24	31
	类型	选项长度	填充长度	保留	
	序列号				
	CGA 参数				
	填充				
类型	8 比特无符号整数，值为 TBD3，表示该选项为 CGA 参数。				
选项长度	8 比特无符号整数，以字节为单位，包括类型、选项长度、填充长度、保留、序列号、CGA 参数以及填充部分。				
填充长度	8 比特无符号整数，表示填充字段的长度，单位为字节。				
保留	8 比特字段，留待将来使用。发送时该字段必须置为 0，且接收者必须忽略该字段。				
序列号	32 比特整数，用于防止重放攻击。如果该 CGA 参数用于响应 CGA 请求，这个字段的值为 CGA 请求中的序列号值加 1；否则，该字段置为 0。				
CGA 参数	该部分长度可变，包含 CGA 参数，参数格式由 IETF RFC 3972 中第 2 章定义。				
填充	可变长度字段，填充的字节数为“填充长度”字段所表示的长度。用于使 CGA 头的长度为 8 字节的整数倍。发送时该字段必须置为 0，且接收者必须忽略该字段。				

6.3 密码生成地址签名扩展头格式

该选项用于发送使用CGA参数中的公钥所对应的私钥对数据包的签名，格式如下：

	0	8	16	24	31
	类型	选项长度	填充长度	保留	
	数字签名				
	填充				
类型	8 比特无符号整数，值为 TBD4，表示该字段为 CGA 签名。				
选项长度	8 比特无符号整数，以字节为单位，包括类型、长度、填充长度、保留、签名以及填充部分。				
填充长度	8 比特无符号整数，以字节为单位。				
保留	8 比特字段，留待将来使用。这个字段必须设为 0。				
数字签名	可变长度字段，是使用与同一个扩展头中的 CGA 参数选项中的公钥对应私钥对数据包部分内容的签名。				
填充	可变长度字段，填充的字节数为：“填充长度”字段所表示的长度。用于使 CGA 头的长度为 8 字节的整数倍。发送时该字段必须置为 0，且接收者必须忽略该字段。				

7 数据包处理规则

CGA请求选项的处理比较简单。当主机需要发送包含CGA 请求选项的数据包时，只需要产生32比特的随机数作为序列号，按照6.1所示包格式封装参数。当主机收到CGA请求选项时，如果选择响应该请求，则提取序列号，用于生成CGA参数选项使用；如果选择不响应该请求，则忽略收到的CGA请求选项。是否响应CGA请求，由主机或上层策略决定。下面的内容主要对包含CGA参数和CGA签名选项的数据包的进入和外出处理规则进行说明。

7.1 数据包发送处理规则

节点发现收到的IPv6数据包的包头中包含了CGA请求选项时，必须在向对方发送的数据包中携带CGA参数和CGA签名选项；节点也可以主动在发出的数据包中加入CGA头，这由上层应用进行选择。

如果节点发送CGA头是作为对CGA 请求的响应，则CGA 参数选项的序列号为CGA请求选项中序列号的值加1；如果节点主动发出CGA参数，那么CGA参数选项中的序列号字段置0。

CGA参数的产生过程见IETF RFC 3972中第4章。

CGA 签名选项中的签名使用的私钥必须与同一个扩展头中的CGA 参数选项中的公钥对应。首先将下列内容按从左到右的顺序串联起来：

- 1) 从 IP 数据包的报头信息中得到的 128 位源地址；
- 2) 从 IP 数据包的报头信息中得到的 128 位目的地址；
- 3) 除了 CGA 签名选项的 CGA 头；
- 4) CGA 头右侧的 IP 数据包有效载荷部分。

对串联得到的数据用SHA-1哈希后，使用RSASSA-PKCS1-v1_5计算签名，并将签名放入CGA 签名选项的数字签名字段。

7.2 数据包接收处理规则

节点接收来自发送方的携带 CGA 扩展头的 IPv6 数据包时，在网络层对 CGA 扩展头进行处理。节点从数据包中获得 CGA 扩展头，包括 CGA 参数和签名。并且可以根据这些信息对数据包的源地址进行验证。验证通过，则对数据包进行下一步的处理，即向上层传输去除 CGA 扩展头的报文。或者也可以忽略该选项，由上层协议决定，即根据相关配置信息，确认是否需要对源地址进行验证。如果节点选择验证，验证步骤如下：

- 1) 如果收到的数据包为 CGA 请求的响应，节点首先将 CGA 参数选项中的序列号减 1，与自己缓存的 CGA 请求中的序列号比较。如果一致，则进行下一步；否则，丢弃该数据包，并发送 ICMP 错误报文。
- 2) 根据 CGA 参数，对 IP 头中包含的源地址进行验证。验证过程见 IETF RFC 3972 中第 5 章。如果验证通过，则进行下一步；否则，丢弃该数据包，发送 ICMP 错误报文。
- 3) 使用 CGA 参数中的公钥对 CGA 签名中的数字签名字段的内容解密，将得到的内容和数据包中部分内容串联（串接方式见 7.1）的哈希值比较。如果内容一致，则验证通过；否则，丢弃该数据包，发送 ICMP 错误报文，通知“验证失败”。

除了上文提到的丢弃数据包的情况以外，以下几种错误也可能会导致数据包的丢弃，并返回ICMP错误报文：

- 1) 扩展头中只出现了 CGA 参数选项而没有 CGA 签名选项；
- 2) 扩展头中只出现了 CGA 签名选项而没有 CGA 参数选项；
- 3) 节点发出了 CGA 请求后，收到的回应数据包中 CGA 头没有包含 CGA 参数和 CGA 签名选项。

8 ICMP 消息

部署和使用CGA头过程中发生某些错误时，需要使用ICMPv6（因为使用的是IPv6协议，所以需用ICMPv6）消息来向源地址报告错误信息。Parameter Problem在ICMPv6中的类型值为4。

8.1 验证失败

YDB 041—2009

验证失败可能由三个方面导致：

- 1) 序列号错误
如果收到的序列号错误，那么就以一定的速率发送类型为 Parameter Problem 的 ICMPv6 消息给对方。Pointer 指向出错的“序列号”字段。
- 2) CGA 验证失败
如果 CGA 验证失败，那么就以一定的速率发送类型为 Parameter Problem 的 ICMPv6 消息给对方。Pointer 要指向“CGA 参数”字段。
- 3) 签名验证失败
如果签名验证失败，那么就以一定的速率发送类型为Parameter Problem的ICMPv6消息给对方。Pointer要指向“数字签名”字段。

8.2 缺少必要选项

缺少必要选项的情况如7.2所述。如果缺少CGA参数选项或CGA签名，则直接向对方发送类型为 Parameter Problem的ICMPv6消息，Pointer指向CGA头，指明其为不识别的IPv6选项。收到此ICMP消息的一方首先需要以一定速率发送CGA签名选项，如果继续收到上述ICMP消息，则再同时发送CGA参数选项和CGA签名。

9 密码生成地址扩展头应用举例

本章内容是在通信过程中使用CGA扩展的一个举例，也是本技术报告推荐的一种部署方案。基本思路为客户端和服务端通过建立TCP连接之前先使用CGA参数完成对对方地址的验证。通信的完整流程如下所示：

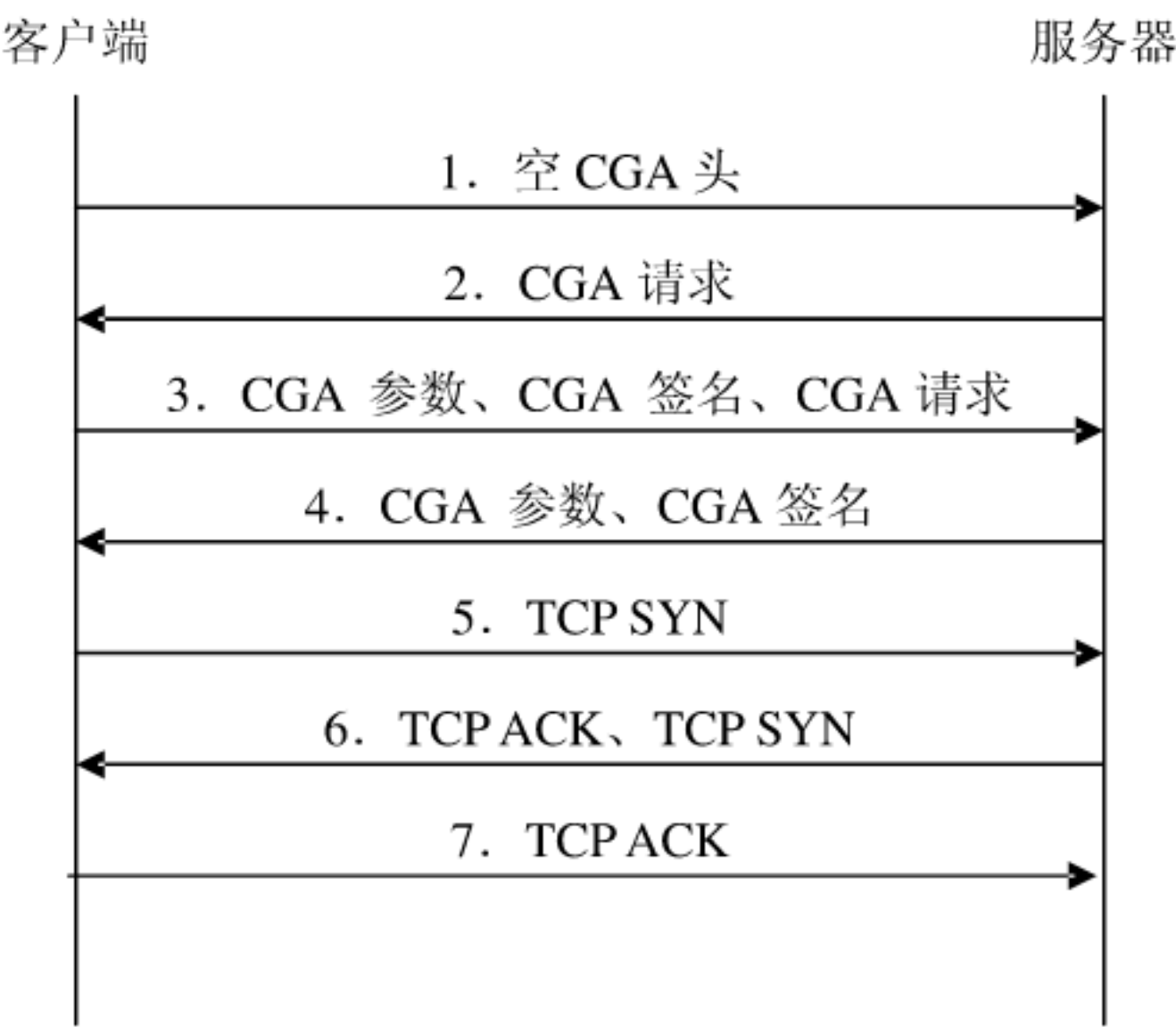


图2 密码生成地址扩展头应用

图 2 为一个 TCP 连接建立的流程，变化在于在建立 TCP 连接之前先使用 CGA 扩展头进行验证。第一条消息中客户端发送一个包含空 CGA 头的数据包表示请求初始化 CGA 验证过程；第二条消息中的 CGA 头包含了一个 CGA 请求选项，请求客户端的 CGA 参数；客户端在第三条消息中包含其 CGA 参数以及 CGA 签名证明地址的真实性，同时发送 CGA 请求消息向服务器请求 CGA 参数和签名；第四条消息包含了服务器的 CGA 参数和 CGA 签名；客户端在验证了服务器的 CGA 参数后，通过第五、第六以及第七条消息，按照标准流程和服务器建立 TCP 连接。

客户端处理流程如下：

- 1) 发送内容为空的 CGA 头；

- 2) 监听端口，接收消息 2；
- 3) 根据消息 2 中的提供 CGA 请求，发送 CGA 参数、CGA 签名以及 CGA 请求，处理规则见 7.1；
- 4) 监听端口，接收消息 4；
- 5) 对消息 4 中服务器提供的 CGA 参数和 CGA 签名进行验证，验证规则见 7.2。如果验证通过，则转到下一步；否则结束通信；
- 6) 通过 TCP 三次握手建立 TCP 连接。

服务器处理流程如下：

- 1) 监听端口，接收消息 1；
- 2) 发送 CGA 请求；
- 3) 监听端口，接收消息 3；
- 4) 对消息 3 中客户端提供的 CGA 参数和 CGA 签名进行验证，验证规则见 7.2。如果验证通过，则转到下一步；否则结束通信；
- 5) 根据消息 3 中的提供 CGA 请求，发送 CGA 参数和 CGA 签名处理规则见 7.1；
- 6) 监听端口，通过TCP三次握手建立TCP连接。

上述的通信流程描述了通信双方为了使用CGA头而进行的相关处理，除此之外，内容还包括了标准的TCP三次握手过程。

10 密码生成地址的产生和配置

10.1 密码生成地址的参数格式

每一个CGA都与一个CGA参数相关，格式如图3。



图3 密码生成地址的参数格式

- 修正符 128 比特的无符号整数，可以是任何值。用来在 CGA 生成的时候执行哈希的扩展和通过给地址增加随机性来增强隐私性。
- 网络前缀 64 比特的网络前缀。

冲突计数	8 比特的无符号整数，取值只能为 0、1 或 2。在 CGA 生成过程中，相同地址检测（见 IETF RFC 3971）检测出冲突的时候，为了解决这个冲突，冲突计数值会增加。
公钥	长度可变的字段，包含地址拥有者的公钥。
扩展域	可选且长度可变的字段，在 IETF RFC 3972 中没有使用。在未来的版本中可能会用该字段作为 CGA 参数数据结构的扩展数据条目。任何不可识别的扩展域数据条目应被忽略。

10.2 参数和地址的生成

CGA 和相关参数应该由如下方法生成：

- 1) 将修正符的值设置为 128 比特随机或伪随机数。
- 2) 将修正符、9 个值为 0 的字节（网络前缀和冲突计数值都设为 0）、公钥、任何可选扩展域从左到右串接起来。对串接起来的值执行 SHA-1 运算，最左边的 112 比特作为 Hash2 的值。
- 3) 将 Hash2 的前 16*Sec（安全参数）比特与 0 比较，如果全为 0（或者 Sec=0）继续下一步，否则将修正符增加 1，返回第 2 步。
- 4) 将 8 比特的冲突计数设为 0。
- 5) 将修正符的终值，网络前缀，冲突计数，公钥和任何可选扩展域从左到右串接，用 SHA-1 算法计算这一比特串。将结果的前 64 比特作为 Hash1 的值。
- 6) Hash1 的值作为接口标识符，并将前 3 比特设为 Sec 的值，设置 6，7 比特为 0。
- 7) 64 比特的网络前缀和 64 比特的接口标识符连接成 128 比特的 IPv6 地址。
- 8) 如果需要的话，执行相同地址检测。如果检测出地址冲突，则将冲突计数加 1 返回第 5 步。当冲突计数为 3 时，停止检测并报告错误。
- 9) 从左到右将修正符的终值，网络前缀，冲突计数的终值，编码的公钥，任何可选的扩展域串起来生成 CGA 参数数据结构。

地址生成算法的输出为一个新的 CGA 和 CGA 参数数据结构。

10.3 配置节点的密码生成地址

如 10.2 所述的 CGA 和 CGA 参数生成方法可以与 DHCPv6 服务器结合，由动态主机配置协议 DHCP 服务器接收客户端（网络节点）发送的配置信息，DHCP 服务器根据接收到的客户端配置，并结合自身的网络配置，为客户端生成 CGA 地址，再将生成的 CGA 地址下发给客户端。结合方式有以下三种：

- 1) 网络节点向其发现的有效 DHCP 服务器发送“请求消息”，该消息中包含公钥和其他由节点指定的 CGA 相关要求参数；接收到该“请求消息”的 DHCP 服务器根据请求消息设置相 CGA 相关设置的 CGA 相关配置，为节点生成 CGA 和 CGA 参数，并在“应答消息”中返回给该网络节点。
- 2) 网络节点向本地链路多播地址发送请求 CGA 相关配置信息的“要求消息”，收到该消息的 DHCP 服务器在“应答消息”中包含 CGA 相关配置信息；网络节点收到后，根据本地的公钥/私钥对，结合 DHCP 服务器应答的 CGA 相关配置信息，计算出 CGA，再发送 DHCP “请求消息”，请求确认该 CGA 是否符合网络配置的要求；如果不符合，则在“应答消息”中包含 CGA 相关配置信息，要求网络节点再次计算 CGA。
- 3) 网络节点根据本地的公钥/私钥对，产生 CGA（子网前缀通过路由广播消息获得），向本地链路多播地址发送 DHCP “要求消息”，其中包含 CGA，并指明请求 DHCP 服务器确认该 CGA 是否符合网络配置的要求；如果不符合，则在“应答消息”中包含 CGA 相关配置信息，要求网络节点再次计算 CGA。

采取上述结合方式生成 CGA 时，DHCPv6 协议需要进行一定的扩展，如在“请求消息”的定义中，添加 CGA 选项的具体规定等。