# Building IPv6 addressing scheme using Hybrid Duplicate Address Detection to prevent Denial of Service Attack

Whenever a host is assigned an IPv6 address, it performs a DAD check to ensure that no other hosts are already using or vying for the same address.

DAD的过程通常包括以下步骤：

* 主机生成一个IPv6地址，并将其标记为“tentative”（临时）状态。
* 主机发送一个邻居发现协议的邻居请求（NS）消息，询问网络上是否有其他设备正在使用这个地址。
* 如果在一定时间内没有收到邻居通告（NA）消息作为响应，或者收到的响应表明没有冲突，那么主机可以确认这个地址是唯一的，并开始使用它。
* 如果收到一个NA消息，表明网络上已经有设备在使用这个地址，主机则必须选择另一个地址或采取其他措施解决冲突。

Static IP address 长期分配给特定设备的IP地址，不会发生变化。

The current defenses against the DAD attack include significant flaws, such as excessive computation, non-scalability, and the need to modify the protocol.

Denial of Service (DoS) and Man-In-The-Middle (MITM) attacks.

Denial of Service (DoS) 攻击

DoS攻击是一种使网络服务不可用的攻击方式。攻击者的目标是使目标服务器、服务或网络无法处理合法用户的请求。这通常是通过以下几种方式实现的：

* 流量过载：攻击者发送大量流量到目标服务器，使其网络带宽饱和，无法处理正常流量。
* 资源耗尽：攻击者利用服务器或服务的特定漏洞，使其消耗过多资源（如CPU、内存），导致无法响应合法请求。
* 服务拒绝：攻击者通过发送特定的请求，使服务崩溃或进入无法处理其他请求的状态。

Man-In-The-Middle (MITM) 攻击

MITM攻击是一种攻击者插入到两个通信方之间的攻击方式。攻击者可以截获、修改和转发通信双方的数据，而通信方可能毫不知情。这种攻击通常涉及以下步骤：

* 拦截通信：攻击者通过各种手段（如伪造Wi-Fi网络）截获两个通信方之间的数据传输。
* 身份伪装：攻击者伪装成合法的通信方，与另一方建立信任关系。
* 数据篡改：攻击者可以读取、修改或注入恶意数据到传输中，而不被通信方察觉。
* 会话劫持：攻击者可能完全接管一个或两个通信方的会话，进行未授权的操作。

For WSN and Mesh-based IoT network requirements

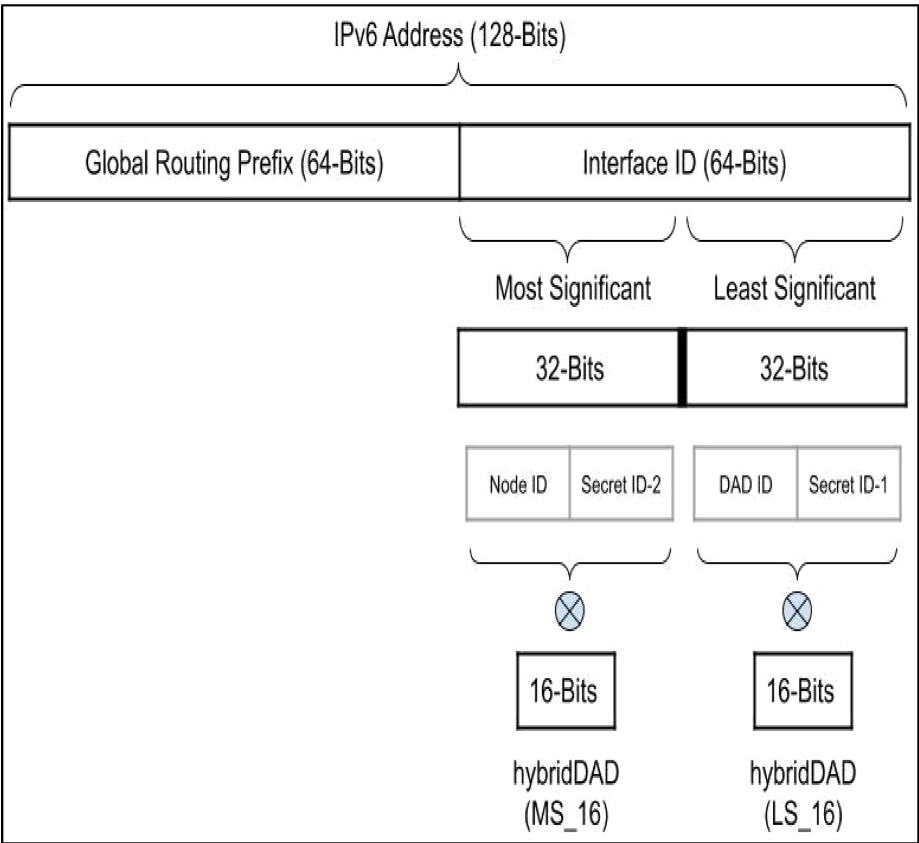
需要考虑WSN和网状IoT网络在设计时需考虑低功耗、自组织、可扩展性等特点

The hybrid DAD method is demonstrated in this study to reduce the DoS attack during the IPv6 setup process in the network. In IPv6, to enhance privacy and security, IP addresses are commonly divided into two parts: the DAD ID (usually the network prefix) and the node ID (often generated from the device's MAC address but can also be randomly generated to improve privacy). This method is known as Privacy Extensions for Addresses, and its purpose is to reduce the risk of exposing user privacy information through IP addresses.

Address predictability: If the node ID is fixed or predictable (such as those based on a MAC address), it allows attackers to more easily guess or track a specific device's IP address. Using randomly generated node IDs can reduce this risk.

Multicast listening: During the Duplicate Address Detection (DAD) process, address queries are completed by sending multicast messages, which may increase the network's attack surface. For example, attackers can listen to these multicast requests to identify new devices in the network or prevent legitimate devices from using their IP addresses by sending false neighbor advertisement messages.

DAD conflicts: Attackers can intentionally respond to all DAD queries in the network, causing address configuration failure. This type of attack is known as a DAD conflict attack.



### IPv6地址结构

IPv6地址总长128位，通常被分为两个64位的部分：

全局路由前缀（Global Routing Prefix, GRP）：64位，用于网络路由。

接口标识符（Interface ID, IID）：64位，用于在本地网络中唯一标识接口。

接口标识符的进一步细分接口标识符进一步被分为两个32位部分：

最高有效位（Most Significant bits, MS-32）

最低有效位（Least Significant bits, LS-32）

这两个部分又各自被分为两个16位部分，用于混合DAD的计算：

LS-32 分为：

DAD ID（16位）

Secret ID-1（16位）

MS-32 分为：

Node ID（16位）

Secret ID-2（16位）

混合DAD值的计算

在进行重复地址检测时，会使用异或（XOR）运算来计算混合DAD值，以提高安全性：

对于邻居请求帧（NS, Neighbor Solicitation）：计算最低有效16位（LS-16），通过对DAD ID和Secret ID-1进行异或（XOR）运算。

对于邻居通告帧（NA, Neighbor Advertisement）：当网络中检测到地址重复时，已建立节点会响应一个携带混合DAD最高有效16位（MS-16）的NA帧。MS-16是通过对Node ID和Secret ID-2进行异或（XOR）运算得到的。这种方法通过使用秘密ID（Secret IDs）和XOR运算，增加了地址配置过程的隐私性和安全性，使得攻击者难以预测或推断出实际的接口标识符。这样的设计可以有效防止一些常见的网络攻击，如地址欺骗和DAD冲突。

假设的IPv6接口标识符（IID）为 0000:8a2e:0370:7334。

MS-32: 0000:8a2e

Node ID: 0000

Secret ID-2: 8a2e

LS-32: 0370:7334

DAD ID: 0370

Secret ID-1: 7334

进行XOR计算

MS-16 (混合): 0000 XOR 8a2e = 8a2e

LS-16 (混合): 0370 XOR 7334 = 7044

算法 1：使用混合DAD过程的IP配置

初始化：hybrid DAD\_count 和 hybrid DAD\_timeout 设为初始值。

生成新IP地址：设备尝试使用 0000:8a2e:0370:7334。

广播NS\_hybrid DAD：设备发送带有混合 LS-16 (7044) 的NS请求。

接收NA\_hybrid DAD：等待网络上其他设备的响应。

循环检测：

如果收到的NA消息是来自一个已经建立的节点，且 MS-16 (8a2e) 匹配，说明地址可能冲突。

如果达到 thresholdDAD（尝试次数上限），并且冲突持续存在，设备会重新生成新的MS位并重复过程。

超时或阈值：如果持续收到冲突响应，或者超时，设备广播网络错误消息并报告失败。

算法 2：验证混合DAD

接收NS\_hybrid DAD：设备接收来自其他设备的NS请求，检查 LS-16。

验证LS-16：

如果 LS-16 (7044) 与本地配置匹配，发送NA\_hybrid DAD响应，表明存在地址冲突。

如果不匹配，丢弃请求并返回失败，表明地址是唯一的。

结果与通讯

如果DAD过程成功，没有冲突，设备将确认其IP地址 0000:8a2e:0370:7334 是唯一的，并用于通信。

如果存在冲突，设备需重新选择Node ID或DAD ID部分，重新计算，直到没有冲突为止。

这个过程确保IPv6地址在网络上的唯一性，避免了地址冲突，同时通过混合DAD的额外安全措施（使用XOR和秘密ID），增加了网络通信的安全性和隐私保护。