Topology Hiding Overview

Topology Hiding is a security function implemented in the application layer on a DSC Node.

Topology Hiding conceals Diameter identity information from all messages leaving a local Realm. Depending on the implementation, general Topology Hiding rules perform the following:

- hide all Diameter host names.
- hide the number of Diameter nodes in a network.

Topology Hiding is applied by a Diameter Edge Agent (DEA) to all messages leaving a protected Realm. The DEA applies Topology Hiding rules to messages based on:

- message connection type and origin.
- application routing rules or criteria such as: Application-ID, Origin-Realm, Origin-Host, Destination-Realm, and Destination-Host.

The Topology Hiding mapping function hides routing and identity details of a DSC Node by obscuring the host portion of the diameter ID, leaving the realm portion unchanged. For example, a diameter ID with the name, mme.realm.com, is mapped to the hidden name, foo.realm.com, when the message exits the protected realm.

Other Topology Hiding requirements include the prevention of other networks from discovering the number of Home Subscriber Servers (HSS) in the network and their identity, including:

- the Diameter name in the Origin-Host AVP contained in request messages from HSS to foreign MME.
- the Diameter name in the Origin-Host AVP contained in answer messages from HSS to foreign MME.

Similarly, to prevent other networks from discovering the number of Mobility Management Entities (MMEs) in the network and their identity, topology hiding performs the following:

- hides the Diameter name in the Origin-Host AVP in requests from MME to foreign HSS.
- re-inserts the Host ID in the Destination-Host AVP in requests from foreign HSS to MME.
- hides the Diameter name in the Origin-Host in answer message from MME to foreign HSS.

Topology Hiding is applied to the following Attribute-Value Pairs (AVPs) that are known to contain Diameter IDs:

- Origin-Host
- Destination-Host
- Error Reporting-Host
- Route Record
- Proxy-Host (within a Proxy-info)
- Session ID (with additional data after the Diameter ID)

For information on provisioning a Topology Hiding configuration on a DSC Node, see sections, Configuring Topology Mapping Tables and Mapping Record and Configuring Topology Mapping Tables and Mapping Record.

**Note**
DSC Topology Hiding supports One-to-One (1:1) and One-to-N (1:N) Topology Mapping configurations.

**Note**
Topology Mapping is a licensed feature that is not included in the base DSC software.
A local DEA performs Topology Hiding for an adjacent local realm. The following figure shows a local DEA performing Topology Hiding for a local realm.

**Figure 1:** Topology Hiding at a DEA and Reverse Mapping

---

**Caution**
Topology Mapping does not function on Diameter hosts that reside in non-adjacent Realms. For this release, Topology Mapping configurations are supported on ADNs in the protected Realm.
A local DEA performs Topology Hiding for the adjacent protected realm. A typical network configuration implements the DEA in the protected realm and hides DSC Node names in messages that leave the realm. The following figure shows a local DEA configuration and an adjacent protected realm.

**Figure 2: Topology Hiding With a Different DEA Realm From the Protected Realm**

An IPX, acting as a local DEA, performs Topology Hiding for several adjacent protected realms. The following figure shows a local IPX configuration and two adjacent protected realms.

**Figure 3: Topology Hiding at an IPX for Adjacent Protected Realms**

**Note**

This release does not support an IPX that provides Topology Hiding for non-adjacent realms.

**Topology Hiding and Routing Tables**

The Topology Hiding Mapping table is applied on a DSC Node after any explicit routing tables. Reverse mapping is applied to message requests entering the DSC Node before explicit routing table rules are applied. Routing tables process unhidden Diameter names.