IPv6 Neighbor Discovery Multicast Suppress

IPv6 Neighbor Discovery (ND) Multicast Suppress suppresses the ND multicast Neighbor Solicit (NS) messages, by either dropping it (and responding to solicitations on behalf of the targets) or converting it into unicast traffic. The conversion of multicast traffic into unicast traffic is performed by replacing a Layer-2 Multicast Destination MAC with a Layer- 2 Unicast Destination MAC. This requires the knowledge of addresses on the link and their binding to the Layer-2. The multicast messages suppressed are Neighbor Solicitation (NS) messages.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

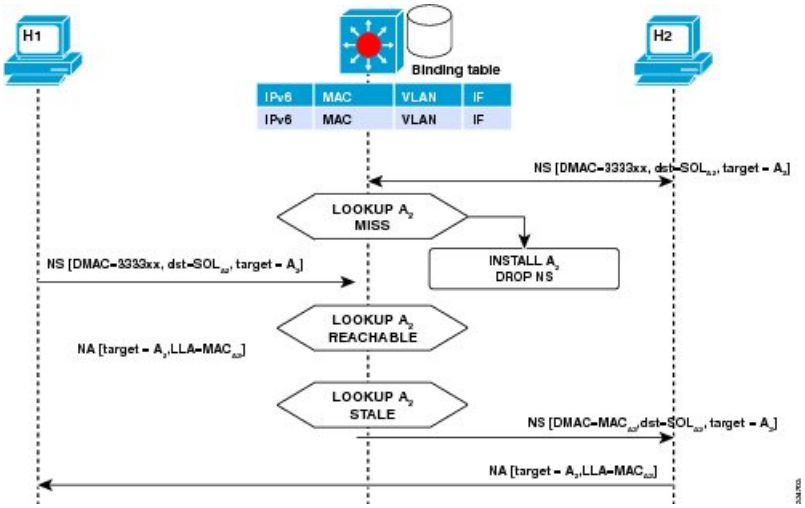
Information About IPv6 Neighbor Discovery Multicast Suppress

Overview of IPv6 Neighbor Discovery Multicast Suppress

The IPv6 Neighbor Discovery (ND) multicast suppress feature stops the ND multicast Neighbor Solicit (NS) messages by dropping them (and responding to solicitations on behalf of the targets) or by converting them into unicast traffic. This feature reduces the amount of control traffic necessary for proper link operations.

When an address is inserted into the binding table, an address resolution request sent to a multicast address is intercepted, and the device either responds on behalf of the address owner or converts the request into a unicast message and forwards it to its destination.

The following figure provides an overview of this feature:



How to Configure IPv6 Neighbor Discovery Multicast Suppress

Configuring IPv6 Neighbor Discovery Multicast Suppress on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy** *policy-name*
4. **[no] mode mc-proxy**
5. **[no] mode full-proxy**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd suppress policy** *policy-name* **Example:**	Specifies a name for the Neighbor Discovery (ND) suppress policy to be configured.

	Command or Action	Purpose
	`Device (config)# ipv6 nd suppress policy policy1` `Device (config-nd-suppress)#`	
Step 4	**[no] mode mc-proxy** **Example:** `Device (config-nd-suppress)# mode mc-proxy`	Specifies if the ND suppress must proxy all multicast Neighbor Solicitation (NS) messages.
Step 5	**[no] mode full-proxy** **Example:** `Device (config-nd-suppress)# mode full-proxy`	Specifies if the ND suppress must proxy both unicast and multicast NS messages.
Step 6	**end** **Example:** `Device (config-nd-suppress)# end`	Exits the ND suppress mode and returns to privileged EXEC mode.

Configuration Examples for IPv6 Neighbor Discovery Multicast Suppress

Example: Configuring IPv6 Neighbor Discovery Suppress on an Interface

```
Device> enable
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy policy1
```

Additional References for IPv6 Neighbor Discovery Multicast Suppress

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Neighbor Discovery Multicast Suppress

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IPv6 Neighbor Discovery Multicast Suppress

Feature Name	Releases	Feature Information
IPv6 Neighbor Discovery Multicast Suppress	15.0(2)SE 15.1(2)SG	IPv6 Neighbor Discovery (ND) Multicast Suppress feature suppresses the ND multicast Neighbor Solicit (NS) messages, by either dropping it (and responding to solicitation on behalf of targets) or converting it into unicast traffic. The conversion of multicast traffic into unicast traffic is performed by replacing a Layer 2 Multicast Destination MAC with a Layer 2 Unicast Destination MAC. This requires the knowledge of addresses on the link and their binding to Layer 2. The multicast messages suppressed are NS messages. The following commands were introduced or modified: **ipv6 nd suppress attach-policy**, **ipv6 nd suppress policy**.
IPv6 Neighbor Discovery Multicast Suppress with DAD Proxy	15.1(2)SG	IPv6 Duplicate Address Detection (DAD) Proxy feature responds to the DAD queries on behalf of a node that owns the queried address. It is useful in environments where nodes cannot communicate directly on the link. The following commands were introduced or modified: **ipv6 nd dad-proxy**, **mode dad-proxy**, **mode md-proxy**.