Contents

ND attack defense commands

Source MAC consistency check commands

ipv6 nd check log enable

Use **ipv6 nd check log enable** to enable the ND logging feature.

Use **undo ipv6 nd check log enable** to restore the default.

Syntax

ipv6 nd check log enable

undo ipv6 nd check log enable

Default

The ND logging feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The ND logging feature logs source MAC inconsistency events, and sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable the ND logging feature to avoid excessive ND logs.

Examples

Enable the ND logging feature.

```
<Sysname> system-view
[Sysname] ipv6 nd check log enable
```

Related commands

ipv6 nd mac-check enable

ipv6 nd mac-check enable

Use **ipv6 nd mac-check enable** to enable source MAC consistency check for ND messages.

Use **undo ipv6 nd mac-check enable** to disable source MAC consistency check for ND messages.

Syntax

ipv6 nd mac-check enable

undo ipv6 nd mac-check enable

Default

Source MAC consistency check for ND messages is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to enable source MAC consistency check on a gateway. The gateway checks the source MAC address and the source link-layer address for consistency for each ND message. If an inconsistency is found, the gateway drops the ND message.

Examples

Enable source MAC consistency check for ND messages.

```
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

ND attack detection commands

display ipv6 nd detection statistics

Use **display ipv6 nd detection statistics** to display statistics for ND messages dropped by ND attack detection.

Syntax

display ipv6 nd detection statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays statistics for ND messages dropped by ND attack detection on all interfaces.

Examples

Display statistics for all ND messages dropped by ND attack detection.

```
<Sysname> display ipv6 nd detection statistics
ND packets dropped by ND detection:
Interface        Packets dropped
GE1/0/1          78
GE1/0/2          0
GE1/0/3          0
GE1/0/4          0
```

Table 1 Command output

Field	Description
Interface	Input interface of the ND messages.
Packets dropped	Number of ND messages dropped by ND attack detection.

ipv6 nd detection enable

Use **ipv6 nd detection enable** to enable ND attack detection. This feature checks the ND message validity.

Use **undo ipv6 nd detection enable** to disable ND attack detection.

Syntax

ipv6 nd detection enable

undo ipv6 nd detection enable

Default

ND attack detection is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ND attack detection for VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] ipv6 nd detection enable
```

ipv6 nd detection trust

Use **ipv6 nd detection trust** to configure an interface as an ND trusted interface.

Use **undo ipv6 nd detection trust** to restore the default.

Syntax

ipv6 nd detection trust

undo ipv6 nd detection trust

Default

All interfaces are ND untrusted interfaces.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ND trusted interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd detection trust
```

Configure Bridge-Aggregation 1 as an ND trusted interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd detection trust
```

reset ipv6 nd detection statistics

Use **reset ipv6 nd detection statistics** to clear ND attack detection statistics.

Syntax

reset ipv6 nd detection statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears ND attack detection statistics for all interfaces.

Examples

Clear all ND attack detection statistics.

```
<Sysname> reset ipv6 nd detection statistics
```

RA guard commands

display ipv6 nd raguard policy

Use **display ipv6 nd raguard policy** to display the RA guard policy configuration.

Syntax

display ipv6 nd raguard policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies an RA guard policy by its name. The policy name is a case-sensitive string of 1 to 31 characters. If you do not specify a policy, this command displays the configuration of all RA guard policies.

Examples

Display the configuration of all RA guard policies.

```
<Sysname> display ipv6 nd raguard policy
Total number of policies: 2
RA Guard policy: policy1
  if-match ACL 2001
  if-match autoconfig managed-address-flag on
  if-match autoconfig other-flag off
  if-match hop-limit maximum 128
  if-match hop-limit minimum 100
  if-match prefix ACL name aa
  if-match router-preference medium
  applied to VLAN 1-3 7
RA Guard policy: policy2
  if-match ACL name zdd
  if-match prefix ACL 2200
```

Table 2 Command output

Field	Description
RA Guard policy	Name of the RA guard policy.
if-match ACL	Number of the ACL in the ACL match criterion.
if-match ACL name	Name of the ACL in ACL match criterion.
if-match autoconfig managed-address-flag	Match criterion of the advertised M flag: • **on**—The value of the advertised M flag is 1. • **off**—The value of the advertised M flag is 0.
if-match autoconfig other-flag	Match criterion of the advertised O flag: • **on**—The value of the advertised O flag is 1. • **off**—The value of the advertised O flag is 0.
if-match hop-limit maximum	The maximum advertised hop limit match criterion.
if-match hop-limit minimum	The minimum advertised hop limit match criterion.
if-match prefix ACL	Number of the ACL used to identify the prefix match criterion.
if-match prefix ACL name	Name of the ACL used to identify the prefix match criterion.
applied to VLAN	ID of the VLAN to which the RA guard policy is applied.

Related commands

ipv6 nd raguard policy

display ipv6 nd raguard statistics

Use **display ipv6 nd raguard statistics** to display RA guard statistics.

Syntax

display ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays RA guard statistics for all interfaces.

Examples

Display RA guard statistics.

```
<Sysname> display ipv6 nd raguard statistics
RA messages dropped by RA guard:
Interface    Dropped
GE1/0/1      78
GE1/0/2      0
GE1/0/3      32
GE1/0/4      0
```

Table 3 Command output

Field	Description
Interface	Interface that received the dropped RA messages.
Dropped	Number of RA messages dropped on the interface.

Related commands

ipv6 nd raguard log enable

reset ipv6 nd raguard statistics

if-match acl

Use **if-match acl** to specify an ACL match criterion.

Use **undo if-match acl** to delete the ACL match criterion.

Syntax

if-match acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match acl

Default

No ACL match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

name *ipv6-acl-name*: Specifies an IPv6 basic ACL by its name, a case-insensitive string of 1 to 63 characters. The name must start with an English letter. To avoid confusion, the name cannot be **all**.

Usage guidelines

RA guard uses the ACL match criterion to match the IP address of the RA message sender. If the sender IP address matches a permit rule, the message passes the check.

If the specified ACL does not exist or does not contain a rule, the ACL match criterion does not take effect.

Examples

Use IPv6 basic ACL 2001 as the ACL match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match acl 2001
```

if-match autoconfig managed-address-flag

Use **if-match autoconfig managed-address-flag** to specify an M flag match criterion.

Use **undo if-match autoconfig managed-address-flag** to delete the M flag match criterion.

Syntax

if-match autoconfig managed-address-flag { **off** | **on** }

undo if-match autoconfig managed-address-flag

Default

No M flag match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

off: Specifies the advertised M flag as 0

on: Specifies the advertised M flag as 1.

Usage guidelines

The M flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain an IPv6 address.

- If the M flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the M flag is set to 0, the host uses stateless autoconfiguration. In stateless autoconfiguration, the host generates an IPv6 address according to its link-layer address and the prefix information in the RA message.

Examples

Specify **on** as the M flag match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match autoconfig managed-address-flag on
```

if-match autoconfig other-flag

Use **if-match autoconfig other-flag** to specify an O flag match criterion.

Use **undo if-match autoconfig other-flag** to delete the O flag match criterion.

Syntax

if-match autoconfig other-flag { **off** | **on** }

undo if-match autoconfig other-flag

Default

No O flag match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

off: Specifies the advertised O flag as 0.

on: Specifies the advertised O flag as 1.

Usage guidelines

The O flag in an RA message determines whether a receiving host uses stateful autoconfiguration to obtain configuration information other than IPv6 address.

- If the O flag is set to 1, the host uses stateful autoconfiguration, for example, uses a DHCPv6 server.
- If the O flag is set to 0, the host uses stateless autoconfiguration.

Examples

Specify **on** as the M flag match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match autoconfig other-flag on
```

if-match hop-limit

Use **if-match hop-limit** to specify a maximum or minimum hop limit match criterion.

Use **undo if-match hop-limit** to delete the maximum or minimum hop limit match criterion.

Syntax

if-match hop-limit { **maximum** | **minimum** } *limit*

undo if-match hop-limit { **maximum** | **minimum** }

Default

No maximum or minimum hop limit match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

maximum: Specifies the maximum advertised hop limit. An RA message passes the check if its current hop limit is not higher than the maximum advertised hop limit.

minimum: Specifies the minimum advertised hop limit. An RA message passes the check if its current hop limit is not less than the minimum advertised hop limit.

limit: Specifies the advertised hop limit in the range of 1 to 255.

Usage guidelines

If a hop limit match criterion is set, and the RA message's current hop limit is 0, the message will be dropped.

Examples

Set the maximum hop limit match criterion to 128 for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match hop-limit maximum 128
```

if-match prefix

Use **if-match prefix** to specify a prefix match criterion.

Use **undo if-match prefix** to delete the prefix match criterion.

Syntax

if-match prefix acl { *ipv6-acl-number* | **name** *ipv6-acl-name* }

undo if-match prefix acl

Default

No prefix match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic ACL by its number in the range of 2000 to 2999.

name *ipv6-acl-name*: Specifies an IPv6 basic ACL by its name, a case-insensitive string of 1 to 63 characters. The name must start with an English letter. To avoid confusion, the name cannot be **all**.

Usage guidelines

An RA message passes the check if the advertised prefixes in the message match the prefixes set by the ACL.

If the specified ACL does not exist or does not contain a rule, the prefix match criterion does not take effect.

Examples

Use IPv6 basic ACL 2000 as the prefix match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 64
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 64
[Sysname-acl-ipv6-basic-2000] rule deny source any
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match prefix acl 2000
```

if-match router-preference

Use **if-match router-preference maximum** to specify a router preference match criterion.

Use **undo if-match router-preference maximum** to delete the router preference match criterion.

Syntax

if-match router-preference maximum { **high** | **low** | **medium** }

undo if-match router-preference maximum

Default

No router preference match criterion exists.

Views

RA guard policy view

Predefined user roles

network-admin

Parameters

high: Sets the maximum router preference to **high**. An RA message passes the check if its router preference is not higher than **high**.

low: Sets the maximum router preference to **low**. An RA message passes the check if its router preference is not higher than **low**.

medium: Sets the maximum router preference to **medium**. An RA message passes the check if its router preference is not higher than **medium**.

Usage guidelines

A host selects a router as the default gateway according to the router preference in received RA messages. If router preferences are the same, the host selects the default router from which the first RA message is received.

An RA message will not pass the router preference check if the message does not have a preference value. This RA message will be dropped.

Examples

Specify **medium** as the router preference match criterion for the RA guard policy **policy1**.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match router-preference maximum medium
```

ipv6 nd raguard apply policy

Use **ipv6 nd raguard apply policy** to apply an RA guard policy to a VLAN.

Use **undo ipv6 nd raguard apply policy** to remove the RA guard policy from a VLAN.

Syntax

ipv6 nd raguard apply policy [*policy-name*]

undo ipv6 nd raguard apply policy

Default

No RA guard policy is applied to a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an RA guard policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a policy, RA guard blocks RA messages on all interfaces in the VLAN except interfaces that are defined to be connected to routers.

Usage guidelines

If an RA message has multiple VLAN tags, RA guard uses the outermost VLAN tag to select the applied RA guard policy.

If the specified RA guard policy does not exist, the command does not take effect.

Examples

Apply the RA guard policy **policy1** to VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] ipv6 nd raguard apply policy policy1
```

Related commands

ipv6 nd raguard policy

ipv6 nd raguard log enable

Use **ipv6 nd raguard log enable** to enable the RA guard logging feature.

Use **undo ipv6 nd raguard log enable** to disable the RA guard logging feature.

Syntax

ipv6 nd raguard log enable

undo ipv6 nd raguard log enable

Default

The RA guard logging feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command allows a device to generate logs when it detects forged RA messages. The log information helps administrators locate and solve problems. Each log records the following information:

- Name of the interface that received the forged RA message.
- Source IP address of the forged RA message.
- Number of RA messages dropped on the interface.

The RA guard logging feature sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable the RA guard logging feature.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard log enable
```

Related commands

display ipv6 nd raguard statistics

reset ipv6 nd raguard statistics

ipv6 nd raguard policy

Use **ipv6 nd raguard policy** to create an RA guard policy and enter its view, or enter the view of an existing RA guard policy.

Use **undo ipv6 nd raguard policy** to delete an RA guard policy.

Syntax

ipv6 nd raguard policy *policy-name*

undo ipv6 nd raguard policy *policy-name*

Default

No RA guard policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Assigns a name to the RA guard policy. The name is a case-sensitive string of 1 to 31 characters.

Examples

Create RA guard policy **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1]
```

Related commands

display ipv6 nd raguard policy

ipv6 nd raguard apply policy

ipv6 nd raguard role

Use **ipv6 nd raguard role** to specify the role of the device attached to the interface.

Use **undo ipv6 nd raguard role** to remove the role of the device attached to the interface.

Syntax

ipv6 nd raguard role { **host** | **router** }

undo ipv6 nd raguard role

Default

No role is specified for the device attached to the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

host: Specifies the host role. The interface attached to a host drops all received RA messages.

router: Specifies the router role. The interface attached to a router forwards all received RA messages.

Usage guidelines

Make sure your setting is consistent with the device type. If you are not aware of the attached device type, do not specify a role for the device.

Examples

Specify **host** as the role for the device attached to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd raguard role host
```

reset ipv6 nd raguard statistics

Use **reset ipv6 nd raguard statistics** to clear RA guard statistics.

Syntax

reset ipv6 nd raguard statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears RA guard statistics for all interfaces.

Examples

Clear RA guard statistics.

```
<Sysname> reset ipv6 nd raguard statistics
```

Related commands

display ipv6 nd raguard statistics