Surveillance VLAN

This chapter contains the following sections:

- surveillance-vlan vlan-id, on page 2
- surveillance-vlan enable (Interface), on page 3
- surveillance-vlan cos, on page 4
- surveillance-vlan aging-timeout, on page 5
- surveillance-vlan cos, on page 6
- Surveillance-vlan traffic-source, on page 7
- Show surveillance-vlan, on page 8
- show surveillance-vlan interface, on page 9

surveillance-vlan vlan-id

To globally enable the ASV (Auto Surveillance VLAN) feature and select the surveillance VLAN ID, use the surveillance-vlan command in Global Configuration mode. Use the no form of this command to disable the feature.

Syntax

surveillance-vlan vlan-id *vlan-id*

no surveillance-vlan vlan-id

Parameters

vlan-id—The ID of the surveillance VLAN

Default Configuration

The ASV feature is disabled.

Command Mode

Global Configuration mode

User Guidelines

The VLAN assigned as the ASV must be an existing static VLAN.

When activating the ASV feature, the IGMP and MLD snooping and querier features become enabled on the VLAN and globally (if disabled). In addition, the bridge multicast filtering global setting is enabled (if disabled).

The Surveillance VLAN must be different form the following VLANs:

- Voice VLAN
- Unauthenticated VLAN
- Guest VLAN
- Private VLAN

The command can be used to modify the VLAN ID of an existing ASV VLAN. In this case the user will be prompted to confirm the configuration, as the change of the ASV VLAN ID may cause changes to VLAN membership on interfaces on which ASV is enabled (command surveillance-vlan enable (Interface)).

Example

The following example enables the ASV feature on VLAN 3:

```
switchxxxxxx(config)# surveillance-vlan vlan-id 3
```

surveillance-vlan enable (Interface)

To enable the ASV feature on an interface, use the surveillance-vlan enable Interface Configuration mode command. To disable the feature on an interface, use the no form of this command.

Syntax

surveillance-vlan enable

no surveillance-vlan enable

Default Configuration

The ASV feature is disabled on all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

The ASV feature can only be enabled on interfaces whose Switchport Mode is Access or General.

Access mode should be used for interfaces who will be connected to a single surveillance device.

General mode should be used to interfaces connected to other network nodes that may be then connected to multiple surveillance devices.

If traffic from a source defined as a surveillance source is detected on an interface with the ASV feature enabled, the interface becomes a member in the surveillance VLAN.

The VLAN priority tag of the surveillance traffic forwarded on this interface will be set to the CoS value defined in the surveillance-vlan cos command.

When traffic from the surveillance source stops and the feature aging-timeout elapses, the interface is removed from the surveillance VLAN and resumes its original static VLAN membership.

In access mode, when an interface is added to the surveillance VLAN, it is removed from its original membership while it is a member of the surveillance-VLAN.

In general mode, the surveillance traffic will be routed on the surveillance VLAN while non-surveillance traffic will use the original VLAN membership of the interface.

The feature cannot be enabled on an interface if it is assigned by RADIUS to a VLAN.

Example

The following example enables the ASV feature on gi1/0/2.

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# surveillance-vlan enable
```

surveillance-vlan cos

To define the CoS value for remarking the VLAN Priority tag (CoS) of surveillance traffic detected on interfaces that are enabled, use the surveillance-vlan cos command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan cos *cos*

no surveillance-vlan *cos*

Parameters

- cos—The class of service applied to surveillance traffic. (Range: 0-7)

Default Configuration

By default the surveillance traffic is remarked with CoS 5.

Command Mode

Global Configuration mode

Example

The following example sets the CoS to 3:

```
switchxxxxxx(config)# surveillance-vlan cos 3
```

surveillance-vlan aging-timeout

To configure the aging timeout of surveillance VLAN membership, use the surveillance-vlan aging-timeout command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan aging-timeout minutes

no surveillance-vlan aging-timeout

- minutes—The amount of time after surveillance traffic stops on the interface before the interface is removed from the ASV. (Range: 1-43200)

Parameters

minutes—The amount of time in minutes after surveillance traffic stops on an interface before the interface is removed from the ASV. (Range: 1-43200)

Default Configuration

1440 minutes.

Command Mode

Global Configuration mode

Example

The following example sets the ASV aging timeout to 12 hours:

```
switchxxxxxx(config)# surveillance-vlan aging-timeout 720
```

surveillance-vlan cos

To define the CoS value for remarking the VLAN Priority tag (CoS) of surveillance traffic detected on interfaces that are enabled, use the surveillance-vlan cos command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan cos *cos*

no surveillance-vlan *cos*

Parameters

- cos—The class of service applied to surveillance traffic. (Range: 0-7)

Default Configuration

By default the surveillance traffic is remarked with CoS 5.

Command Mode

Global Configuration mode

Example

The following example sets the CoS to 3:

```
switchxxxxxx(config)# surveillance-vlan cos 3
```

Surveillance-vlan traffic-source

To add a traffic source to be tracked by the ASV feature, use the surveillance-vlan traffic-source command in Global Configuration mode. Use the no form of this command to delete a traffic source from the table.

Syntax

surveillance-vlan traffic-source default | {**mac** *mac-address*|**oui** *OUI*} [**description** description]}

no surveillance-vlan traffic-source {**mac** *mac-address*|**oui** *OUI*}

Parameters

- *mac-address*—A unicast MAC address which would be added to the traffic-source table.
- *oui*—A three octet MAC address prefix which would be added to the traffic-source table.
- *description*—A description of the surveillance traffic source (length: up to 32 characters).

Default Configuration

The table is empty.

Command Mode

Global Configuration mode

User Guidelines

The traffic source table contains MAC and OUI entries. If traffic from a source matching these entries is received on an interface with the ASV feature enabled, the interface will be added to the Auto Surveillance VLAN.

Examples

The following example adds an OUI entry to the table:

```
switchxxxxxx(config)# surveillance-vlan traffic-source oui a0:bb:cc
```

The following example adds a MAC entry to the table with a description:

```
switchxxxxxx(config)# surveillance-vlan traffic-source mac 12:44:4a:4c:13:ec
description floor1_sec
```

The following example deletes a mac based entry from the table:

```
switchxxxxxx(config)# no surveillance-vlan traffic-source mac
12:44:4a:4c:13:ec
```

Show surveillance-vlan

To display the ASV global settings and status and the traffic source table, use the show surveillance-vlan command in Privileged EXEC mode.

Syntax

show surveillance-vlan

Command Mode

Privileged EXEC mode

User Guidelines

The command shows the global settings of the ASV feature and the traffic source table. The traffic source table has the following columns:

- MAC/OUI: The MAC or OUI prefix of this traffic source.
- Description: A description of the traffic source.
- Active: This value is Yes if traffic from this source was detected on any interface with the ASV feature enable that has not timed out due to the aging timeout.
- Interface: A list of interfaces with the ASV feature enabled that detected traffic from this source.

Example

This command shows the global status and configurations of the ASV feature.

The column Active in the Surveillance Traffic Sources table indicates that there is a current flow from this source which is not yet aged out of the FDB. The interfaces column shows the interfaces where traffic matching this source OUI or MAC is currently received.

The following example shows the output of the command:

```
switchxxxxxx# show surveillance-vlan
Surveillance VLAN is enabled on VLAN 5
Aging timeout: 1440 minutes
CoS: 5
Surveillance-Traffic sources
MAC/OUI Description Active Interface
================ =========== ====== =========
00:03:C5 Mobotix Yes ge1/2, LAG8
00:04:7D Pelco No
10:22:33:12:44:22 RND-Server Yes ge1/4
```

show surveillance-vlan interface

This command shows the interface status and configuration related to the ASV feature.

To display the ASV interface settings and status, use the show surveillance-vlan interface command in Privileged EXEC mode.

Syntax

show surveillance-vlan interface

Command Mode

Privileged EXEC mode.

User Guidelines

The command shows the interface settings of the ASV feature on the interfaces of the device.

The settings table has the following columns:

- Interface: The interface whose status the row shows.
- Enabled: A boolean indication on whether the ASV feature is enabled on the interface.
- Active: This value is Yes if the interface became a member of the ASV VLAN (even if the MAC address forwarding table does not include an entry for the surveillance traffic source address).

Example

The following example shows the output of the command:

```
Switchxxxxxx# show surveillance-vlan interface
Interface Enabled Active
========= ======= ======
ge1/1     Yes     No
ge1/2     Yes     Yes
ge1/3     No      No
```