Basic Configuration of Change of Authorization in Catalyst 1300 Switch using CLI

Objective

The objective of this article is to show you how to perform a basic configuration of change of authorization (CoA) feature in Catalyst 1300 switches using the command line interface (CLI).

Applicable Devices and Software Version

- Catalyst 1300 switches | 4.1.3.36

Introduction

Change of Authorization (CoA) is an extension to the RADIUS protocol, that allows you to change the properties of an authentication, authorization, and accounting (AAA) or dot1x user session after it has been authenticated. When a policy for a user or group in AAA changes, administrators can transmit RADIUS CoA packets from the AAA server, such as a Cisco Identity Services Engine (ISE), to reinitialize authentication and apply the new policy.

The Cisco Identity Services Engine (or ISE) is a fully featured Network Based Access Control and Policy Enforcement Engine. It provides security analysis and enforcement, RADIUS and TACACS services, policy distribution, and more. Cisco ISE is currently the only supported CoA Dynamic Authorization Client for Catalyst 1300 switches. Refer to the **ISE Admin guide** for more information.

The CoA support has been added to the Catalyst 1300 switches in firmware version 4.1.3.36. This includes support for disconnecting users and changing authorizations applicable to a user session. The device supports the following CoA actions:

- Disconnect Session
- Disable host port CoA command
- Bounce host port CoA command
- Reauthenticate host CoA command

In this article, you will find the commands for a basic CoA configuration in Catalyst 1300 switches using CLI. The steps could vary based on the user settings and requirements.

Table of Contents

Basic CoA Configuration using CLI

Set Up RADIUS Server and RADIUS Accounting

To configure the RADIUS server, from global config mode, use the following commands:

Step 1

Use the *radius-server key* command to set the authentication key for RADIUS communications between the device and the RADIUS daemon.

```
radius-server key <key-string>
```

Step 2

Use the *radius-server host* command to configure a RADIUS server host.

```
radius-server host<ISE Server IP Address> key <key-string>
priority 1 usage dot1.x
```

- The IP address will be the ISE server IP address.
- *key <key-string>* - Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon.
- *Priority* - Specifies the order in which servers are used, where 0 has the highest priority. (Range:0–65535)
- usage dot1.x - specifies that the RADIUS server is used for 802.1x port authentication.

Step 3

```
aaa accounting dot1x start-stop group radius
```

Configure Dynamic Authorization Server

Step 1

From the global configuration mode, enter the CoA configuration mode by running the command:

```
aaa server radius dynamic-author
```

Step 2

To configure the RADIUS key to be shared between the device and a CoA client (Range: 0–128 characters), use the command *server-key <key-string>* in dynamic authorization local server

configuration mode. The key provided in the CoA request must match this key.

```
server-key <key-string>
```

> **Note:**
> For ISE, the key-string will be the same key string you specified for the RADIUS server key-string when configuring RADIUS.

Step 3

Enter the CoA client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

```
client <ISE Server IP Address>
```

Step 4

```
Exit
```

Configure 802.1x

To enable 802.1X globally, use the *dot1x system-auth-control* command.

```
dot1x system-auth-control
```

Configure 802.1x on a port

Step 1

Enter the Interface configuration and select the interface ID by using the command interface GigabitEthernet<Interface ID>.

```
interface gi1/0/1
```

Step 2

To enable manual control of the port authorization state, use the *dot1x port-control* command. Auto mode enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.

```
dot1x port-control auto
```

Step 3

To initiate manually re-authentication of all 802.1X-enabled ports or the specified 802.1X-

enabled port, use the *dot1x re-authenticate* command in privileged EXEC mode.

```
dot1x re-authenticate gi1/0/1
```

Step 4

To configure the port security learning mode, use the port security mode Interface (Ethernet, Port Channel) configuration mode command. *Secure delete-on-reset* parameter is a secure mode with limited learning secure MAC addresses with the delete-on-reset time-of-live.

```
port security mode secure delete-on-reset
```

Step 5

To exit the interface configuration, enter the following:

```
exit
```

Other Commands for CoA Configuration

Here are some of the other CoA commands that can be used based on your configuration and set up.

- *attribute event-timestamp drop-packet* – This command is used in dynamic authorization local server configuration mode to configure the device to discard a Packet of Disconnect (PoD) request or CoA request that do not include an event-timestamp attribute.

```
attribute event-timestamp drop-packet
```

- *authentication command bounce-port ignore* - To configure the device to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the authentication command bounce-port ignore command in global configuration mode.

```
authentication command bounce-port ignore
```

- *authentication command disable-port ignore* - To configure the device to ignore a RADIUS CoA disable-port command, use this command in global configuration mode.

```
authentication command disable-port ignore
```

- *domain delimiter <character>* - To configure the username domain delimitator for received PoD and CoA requests use the domain delimiter command in dynamic authorization local server configuration mode.

```
domain delimiter $
```

In this example the $ character is configured as a delimiter.

- *domain stripping [right-to-left]* - To enable and define the behavior for username domain stripping for received PoD and CoA Requests use the domain stripping command in dynamic authorization local server configuration mode.

```
domain stripping right-to-left
```

- ignore server-key – This command is used in dynamic authorization local server configuration mode to configure the device to ignore the CoA server-key.

```
ignore server-key
```

CLI Commands in Privilege Exec Mode

From privilege exec mode, you can run show commands on the authenticated clients, clear the client counters, and show Dynamic Authorization Server configuration.

- Use the *show aaa clients* to show AAA (CoA) client's statistics.

```
show aaa clients
```

- Use the *show aaa server radius dynamic-author* command to show CoA configuration.

```
show aaa server radius dynamic-author
```

- *clear aaa counters* can be used to clear the aaa clients counters

```
clear aaa clients counters
```

Conclusion

You have now completed a basic change of authorization (CoA) configuration in Catalyst 1300 switch using CLI.

For more information on the CLI commands for the Catalyst 1300 switches, refer to the **Cisco Catalyst 1300 Switches Series CLI Guide**.