CHAPTER 13

Configuring Auto Smartports Macros

This chapter describes how to configure Auto Smartports macros.

Unless otherwise noted, the term *switch* refers to a standalone switch and a switch stack.

The Catalyst 2960 switch command reference has command syntax and usage information.

This chapter contains these sections

- Understanding Auto Smartports and Static Smartports Macros, page 13-1
- Configuring Auto Smartports, page 13-3
- Configuring Static Smartports Macros, page 13-17
- Displaying Auto Smartports and Static Smartports Macros, page 13-20

Understanding Auto Smartports and Static Smartports Macros

Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate Auto Smartports macro on the port. When there is a link-down event on the port, the switch removes the macro. For example, when you connect a Cisco IP phone to a port, Auto Smartports automatically applies the IP phone macro. The IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic. Auto Smartports uses event triggers to map devices to macros.

The Auto Smartports macros embedded in the switch software are groups of CLI commands. The CISCO_PHONE event detected on a port triggers the switch to apply the commands in the CISCO_PHONE_AUTO_SMARTPORT macro. You can also create user-defined macros by using the Cisco IOS Shell scripting capability, which is a BASH-like language syntax for command automation and variable replacement.

Auto Smartports macros differ from static Smartports macros because static Smartports macros provide port configuration that you manually apply based on the device connected to the port. When you apply a static Smartports macro the CLI commands within the macro are added to the existing port configuration. When there is a link-down event on the port, the switch does not remove the static macro configuration.

Auto Smartports uses events to map macros to the source port of the event. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from a connected device. The detection of a device invokes a CDP event trigger: Cisco IP Phone, Cisco Wireless Access Point including Autonomous and Lightweight Access Points, Cisco switch, Cisco router, and Cisco IP Video Surveillance Camera.

Additional event triggers for Cisco and third-party devices are user-defined MAC-address groups, MAC authentication bypass (MAB) messages, 802.1x authentication messages, and Link Layer Discovery Protocol (LLDP) messages.

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP-supported devices use TLVs to receive and send information. This protocol advertises details such as configuration information, device capabilities, and device identity. Auto Smartports uses the LLDP *system capabilities* TLV as the event trigger. For more information about configuring the LLDP system capabilities TLV attributes for Auto Smartports, see Chapter 27, "Configuring LLDP, LLDP-MED, and Wired Location Service."

For devices that do not support CDP, MAB, or 802.1x authentication, such as network printers, LLDP, or legacy Cisco Digital Media Players, you can configure a MAC-address group with a MAC operationally unique identifier (OUI)-based trigger. You map the MAC-address to a built-in or user-defined macro containing the desired configuration.

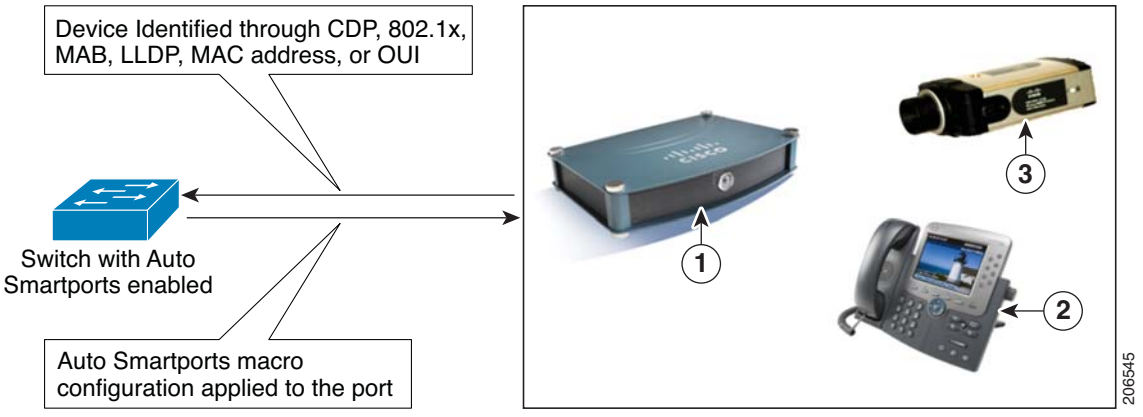
You can designate a remote server location for user-defined macro files. You can then update and maintain one set of Auto Smartport macro files for use by multiple switches across the network.

The Auto Smartports macro persistent feature enables macro configurations to remain applied on the switch ports regardless of a detected linkdown event. You can use this feature to make the Auto Smartport macros configurations static on the switch. This can eliminate multiple system log and configuration change notification events when the switch has linkup and linkdown events or is a participating entity in an EnergyWise-configured network.

Auto Smartports and Cisco Medianet

Cisco Medianet enables intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports. The switch identifies Cisco and third-party video devices by using CDP, 802.1x, MAB, LLDP, and MAC addresses (Figure 13-1). The switch applies the applicable Auto Smartports macro to enable the appropriate VLAN and QoS settings for the device. The switch also uses a built-in MAC-address group to detect the legacy Cisco DMP, based on an OUI of of4400 or 23ac00. You can also create custom user-defined macros for any video device.

Figure 13-1 Cisco Medianet Deployment Example



Configuring Auto Smartports

- Default Auto Smartports Configuration, page 13-3
- Auto Smartports Configuration Guidelines, page 13-4
- Enabling Auto Smartports, page 13-5
- Configuring Auto Smartports Default Parameter Values, page 13-5
- Configuring Auto Smartports MAC-Address Groups, page 13-7
- Configuring Auto Smartports Macro Persistent, page 13-8
- Configuring Auto Smartports Built-In Macro Options, page 13-9
- Creating User-Defined Event Triggers, page 13-12
- Configuring Auto Smartports User-Defined Macros, page 13-15

Default Auto Smartports Configuration

- Auto Smartports is disabled globally and enabled per interface.
- CDP fallback is disabled globally and enabled per interface.
- Cisco IOS shell is enabled.
- Auto Smartports macros are used by default when ASP is enabled for the devices shown in Table 13-1.

Table 13-1 Auto Smartports Built-In Macros

Macro Name	Description
CISCO_PHONE_AUTO_ SMARTPORT	This macro applies the IP phone macro for Cisco IP phones. It enables QoS, port-security, storm-control, DHCP snooping, and spanning-tree protection. It also configures the access and voice VLANs for that interface.
CISCO_SWITCH_AUTO_ SMARTPORT	This macro applies the switch macro for Cisco switches. It enables QoS and trunking with 802.1Q encapsulation. It also configures the native VLAN on the interface.
CISCO_ROUTER_AUTO_ SMARTPORT	This macro applies the router macro for Cisco routers. It enables QoS and trunking with 802.1Q encapsulation, and spanning-tree BPDU protection.
CISCO_AP_AUTO_ SMARTPORT	This macro applies the wireless access point macro for Cisco APs. It enables QoS and trunking with 802.1Q encapsulation. It also configures the native VLAN on the interface.
CISCO_LWAP_AUTO_ SMARTPORT	This macro applies the light-weight wireless access point macro for Cisco light-weight wireless access points. It enables QoS, port security, storm control, DHCP snooping, and spanning-tree protection. It configures the access VLAN for the interface and provides network protection from unknown unicast packets.
CISCO_IPVSC_AUTO_ SMARTPORT	This macro applies the IP camera macro for Cisco IP video surveillance cameras. It enables QoS trust, port security, and spanning-tree protection. It configures the access VLAN for the interface and provides network protection from unknown unicast packets.
CISCO_DMP_AUTO_ SMARTPORT	This macro applies the digital media player macro for Cisco digital media players. It enables QoS trust, port security, and spanning-tree protection. It configures the access VLAN for the interface and provides network protection from unknown unicast packets.

Auto Smartports Configuration Guidelines

- The built-in macros cannot be deleted or changed. However, you can override a built-in macro by creating a user-defined macro with the same name. To restore the original built-in macro, delete the user-defined macro.
- If you enable both the **macro auto device** and the **macro auto execute** global configuration commands, the parameters specified in the command last executed will be applied to the switch. Only one command is active on the switch.
- To avoid system conflicts when Auto Smartports macros are applied, remove all port configuration except for 802.1x authentication.
- Do not configure port security when enabling Auto Smartports on the switch.
- If the macro conflicts with the original configuration, the macro will not apply some of the original configuration commands, or the antimacro will not remove them. (The antimacro is the portion of the applied macro that removes the macro at a link-down event.)

  For example, if 802.1x authentication is enabled, you cannot remove switchport-mode access configuration. Remove the 802.1x authentication before removing the switchport mode configuration.
- A port cannot be a member of an EtherChannel when you apply Auto Smartports macros. If you use EtherChannels, disable Auto Smartports on interfaces that are members of the EtherChannels by using the **no macro auto processing** interface configuration command.
- The built-in macro default data VLAN is VLAN 1. The built-in macro default voice VLAN is VLAN 2. (VLAN 1 is the default data VLAN for all macros. VLAN 2 is the default voice VLAN for all macros.) If your switch uses different access, native, or voice VLANs, use the **macro auto device** or the **macro auto execute** global configuration commands to configure the desired nondefault values.
- Use the **show macro auto device** privileged EXEC command to display the default macros with the default parameter values, current values, and the configurable parameter list for each macro. You can also use the **show shell functions** privileged EXEC command to view the built-in macro default values.
- For 802.1x authentication or MAB, configure the RADIUS server to support the Cisco attribute-value (av) pair **auto-smart-port=***event trigger* to detect non-Cisco devices.
- For stationary devices that do not support CDP, MAB, or 802.1x authentication, such as network printers, you can configure a MAC-address group with a MAC OUI-based trigger and map it to a user-defined macro containing the desired configuration.
- The switch supports Auto Smartport macros only on directly connected devices. Multiple device connections, such as hubs, are not supported. If multiple devices are connected, the macro applied is the one associated with the first device that is detected.
- If authentication is enabled on a port, the switch ignores a MAC-address trigger if authentication fails.
- The order of CLI commands within the macro and the corresponding antimacro can be different.
- Auto SmartPorts does not perform any global configuration. If the interface level Auto Smartport macros require any global configuration, you must manually add the global configuration.

Enabling Auto Smartports

Follow this procedure to enable Auto Smartports macros globally on the switch. This procedure is required. To disable Auto Smartports macros on a specific port, use the **no auto global processing** interface configuration command.

Note Starting from Cisco IOS 15.0(2)SE1 release, enabling autosmart ports will also enable last-resort macro "CISCO_LAST_RESORT_EVENT". This means that ports that go undetected by any predefined macro, will hit last-resort macro and push certain configuration (vlan 1/spanning-tree portfast). If you do not want to have last-resort macro enabled, you will need to explicitly disable it.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto global processing**	Globally enable Auto Smartports on the switch.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify that Auto Smartports is enabled.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no macro auto global processing** global configuration command.

You can use the **show macro auto device**, the **show shell** *functions*, and the **show shell** *triggers* privileged EXEC commands to display the event triggers, the built-in macros, and the built-in macro default values.

This example shows how to enable Auto Smartports on the switch and how to disable the feature on a specific interface:

```
Switch(config)# macro auto global processing
Switch(config)# interface interface_id
Switch(config-if)# no macro auto processing
```

Configuring Auto Smartports Default Parameter Values

The switch automatically maps from event triggers to built-in macros. You can follow this procedure to replace Auto Smartports macro default parameter values with values that are specific to your switch. This procedure is optional.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**show macro auto device**	Display the macro default parameter values.
Step 2	**configure terminal**	Enter global configuration mode.

	Command	Purpose
Step 3	**macro auto device** {**access-point** | **ip-camera** | **lightweight-ap** | **media-player** | **phone** | **router** | **switch**} [*parameter*=*value*]	Replace the specified macro default parameter values. Enter new values in the form of name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...]. Default values are shown for each macro default parameter value. • **access-point NATIVE_VLAN=**1 • **ip-camera ACCESS_VLAN=**1 • **lightweight-ap ACCESS_VLAN=**1 • **media-player ACCESS_VLAN=**1 • **phone ACCESS_VLAN=**1 **VOICE_VLAN=**2 • **router NATIVE_VLAN=**1 • **switch NATIVE_VLAN=**1 **Note** You must enter the correct parameter name (for example, VOICE_VLAN) because this text string must match the text string in the built-in macro definition.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show macro auto device**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no macro auto device** {*macro name*} *parameter*=*value* global configuration command.

This example shows how to view the IP phone macro parameter values and how to change the default voice VLAN to 20. When you change the default values, they are not applied on interfaces that already have applied macros. The configured values are applied at the next link-up event. Note that the exact text string was used for VOICE_VLAN. The entry is case sensitive.

```
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:ACCESS_VLAN=1 VOICE_VLAN=2

Switch# configure terminal
Switch(config)# macro auto device phone VOICE_VLAN=20
Switch(config)# end
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:voice_vlan=20
```

Configuring Auto Smartports MAC-Address Groups

For devices such as printers that do not support neighbor discovery protocols such as CDP or LLDP, use the MAC-address-based trigger configurations for Auto Smartports. This procedure is optional and requires these steps:

- Configure a MAC-address-based trigger by using the **macro auto mac-address** global configuration command.
- Associate the MAC-address trigger to a built-in or a user-defined macro by using the **macro auto execute** global configuration command.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto mac-address-group** *name*	Specify the group name, and enter MAC address configuration mode.
Step 3	[**mac-address list** *list*] | [**oui** [**list** *list* | **range** *word* **size** *number*]]	Configure a list of MAC addresses separated by a space. Specify an operationally unique identifier (OUI) **list** or **range**. The OUI is the first three bytes of the MAC address and identifies the manufacturer of the product. Specifying the OUI allows devices that do not support neighbor discovery protocols to be recognized. • **list**—enter an OUI list in hexadecimal separated by a space. • **range**—Enter the OUI start range in hexadecimal. Enter the size (1–5) to create sequential addresses.
Step 4	**macro auto execute** *address_trigger* **built-in** *macro name*	Map the MAC address-group trigger to a built-in or user-defined macro. The MAC-address trigger is applied to an interface after a hold-time of 65 seconds. The hold time allows for a neighbor discovery protocol such as CDP or LLDP to be used instead of the MAC address.
Step 5	**exit**	Return to configuration mode.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show macro auto address-group**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete an address group, use the **no macro auto mac-address-group** *name* global configuration command. Enter **no macro auto mac-address-group** *name* to remove the macro trigger and any associated trigger mapping to a macro defined by using the **macro auto execute** global configuration command. Entering **no macro auto execute mac-address-group** only removes the mapping of the trigger to the macro.

This example shows how to create a MAC-address-group event trigger called *address_trigger* and how to verify your entries:

```
Switch# configure terminal
Switch(config)# macro auto address-group mac address_trigger
Switch(config-addr-grp-mac)# mac-address list 2222.3333.3334 22.33.44 a.b.c
Switch(config-addr-grp-mac)# oui list 455555 233244
Switch(config-addr-grp-mac)# oui range 333333 size 2
Switch(config-addr-grp-mac)# exit
Switch(config)# mac auto execute address-trigger builtin macro
Switch(config)# exit
```

```
Switch(config)# end
Switch(config)# macro auto execute mac-address-trigger builtin CISCO_PHONE_ATUO_SMARTPORT
Switch(config)# end
Switch# show running configuration | include macro
macro auto mac-address-group address_trigger
mac auto mad-address-group hel
mac auto execute mad-address-trigger builtin CISCO_PHONE_AUTO_SMARTPORT
 macro description CISCO_DMP_EVENT
 mac description CISCO_SWITCH_EVENT
!
<output truncated>
```

Configuring Auto Smartports Macro Persistent

When you enable Auto Smartports on the switch, the default is that the macro configuration is applied at a link-up event and removed at a link-down event. When you enable the macro persistent feature, the configuration is applied at link-up and is not removed at link-down. The applied configuration remains, regardless of link-up or link-down events on the switch. The macro persistent feature remains configured through a reboot if the running configuration file is saved.

Follow this procedure to enable Auto Smartports macros to remain active on the switch after a link-down event. This procedure is optional.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto sticky**	Enable Auto Smartport macro configurations to remain on the interface on a link-down event.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show macro auto**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the Auto Smartports macro persistent feature, use the **no macro auto sticky** global configuration command.

This example shows how to enable the Auto Smartports auto-sticky feature on the switch:

```
Switch(config)# macro auto sticky
```

Configuring Auto Smartports Built-In Macro Options

Use this procedure to map event triggers to built-in macros and to replace the built-in macro default parameter values with values that are specific to your switch. If you need to *replace* default parameters values in a macro, use the **macro auto device** global configuration command. All commands in this procedure are optional.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto execute** *event trigger* **builtin** *built-in macro name* [*parameter=value*] [*parameter=value*]	Define mapping from an event trigger to a built-in macro. Specify an *event trigger*: • CISCO_DMP_EVENT • CISCO_IPVSC_EVENT • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • WORD—Apply a user-defined event trigger. Specify a **builtin** *built-in macro name*: Enter new values in the form of name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...]. Default values are shown exactly as they should be entered. • CISCO_DMP_AUTO_SMARTPORT Specify the parameter values: ACCESS_VLAN=1. • CISCO_IPVSC_AUTO_SMARTPORT Specify the parameter values: ACCESS_VLAN=1. • CISCO_PHONE_AUTO_SMARTPORT Specify the parameter values: ACCESS_VLAN=1 and VOICE_VLAN=2. • CISCO_SWITCH_AUTO_SMARTPORT Specify the parameter values: NATIVE_VLAN=1. • CISCO_ROUTER_AUTO_SMARTPORT Specify the parameter values: NATIVE_VLAN=1. • CISCO_AP_AUTO_SMARTPORT Specify the parameter values: NATIVE_VLAN=1. • CISCO_LWAP_AUTO_SMARTPORT Specify the parameter values: ACCESS_VLAN=1.

	Command	Purpose
Step 3	**remote** *url*	Specify a remote server location for the remote macro file: • The syntax for the local flash file system on the standalone switch or the stack master: **flash:** • The syntax for the local flash file system on a stack member: **flash** *member number***:** • The syntax for the FTP: **ftp:**[[*//username*[**:***password*]*@location*]*/directory*]*/filename* • The syntax for an HTTP server: **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/filename* • The syntax for a secure HTTP server: **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/filename* • The syntax for the NVRAM: **nvram://**[[*username***:***password*]@][*/directory*]*/filename* • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[*//username@location*]*/directory*]*/filename* • The syntax for the Secure Copy Protocol (SCP): **scp:**[[*//username@location*]*/directory*]*/filename* • The syntax for the TFTP: **tftp:** [[*//location*]*/directory*]*/filename*
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	Save your entries in the configuration file.

This example shows how to use two built-in Auto Smartports macros for connecting Cisco switches and Cisco IP phones to the switch. This example modifies the default voice VLAN, access VLAN, and native VLAN for the trunk interface:

```
Switch# configure terminal
Switch(config)#!!! the next command modifies the access and voice vlans
Switch(config)#!!! for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!! the next command modifies the Native vlan used for inter switch trunks
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config)#
Switch(config)#!!! the next command enables auto smart ports globally
Switch(config)# macro auto global processing cdp-fallback
Switch(config)#
Switch(config)# exit

Switch# !!! here's the running configuration of the interface connected
Switch# !!! to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface gigabitethernet0/1
Building configuration...
```

```
Current configuration : 284 bytes
!
 interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

This example shows how to configure the remote macro with the setting for native VLAN 5.

a. Configure the remote macro in the macro.txt file.

b. Use the **macro auto execute** configuration command to specify the remote location for the macro file.

```
if [[ $LINKUP -eq YES ]]; then
    conf t
           interface $INTERFACE
                  macro description $TRIGGER
                  auto qos voip trust
                  switchport trunk encapsulation dot1q
                  switchport trunk native vlan $NATIVE_VLAN
                  switchport trunk allowed vlan ALL
                  switchport mode trunk
            exit
    end
else
    conf t
           interface $INTERFACE
                 no macro description
                 no auto qos voip trust
                 no switchport mode trunk
                 no switchport trunk encapsulation dot1q
                 no switchport trunk native vlan $NATIVE_VLAN
                 no switchport trunk allowed vlan ALL
           exit
    end

Switch(config)# macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt
NATIVE_VLAN=5

Switch# show running configuration | include macro
macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt
NATIVE_VLAN=5
Switch#
```

Creating User-Defined Event Triggers

When using MAB or 802.1x authentication to trigger Auto Smartports macros, you need to create an event trigger that corresponds to the Cisco attribute-value pair (**auto-smart-port**=*event trigger*) sent by the RADIUS server. This procedure is optional.

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**shell trigger** *identifier description*	Specify the event trigger identifier and description. The identifier should have no spaces or hyphens between words.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show shell triggers**	Display the event triggers on the switch.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no shell trigger** *identifier* global configuration command to delete the event trigger.

This example shows how to map a user-defined event trigger called RADIUS_MAB_EVENT to the built-in macro CISCO_AP AUTO_SMARTPORT, replace the default VLAN with VLAN 10, and how to verify the entries.

a. Connect the device to a MAB-enabled switch port.

b. On the RADIUS server, set the attribute-value pair to **auto-smart-port**=RADIUS_MAB_EVENT.

c. On the switch, create the event trigger RADIUS_MAB_EVENT.

d. The switch recognizes the attribute-value pair=RADIUS_MAB_EVENT response from the RADIUS server and applies the macro CISCO_AP_AUTO_SMARTPORT.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# !!! create a user defined trigger and map
Switch(config)# !!! a system defined macro to it
Switch(config)# !!! first create the trigger event
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
Switch(config)#
Switch(config)#!!! map a system defined macro to the trigger event
Switch(config)# macro auto execute RADIUS_MAB_EVENT builtin ?
_ CISCO_DMP_AUTO_SMARTPORT
_ CISCO_IPVSC_AUTO_SMARTPORT
  CISCO_AP_AUTO_SMARTPORT
  CISCO_LWAP_AUTO_SMARTPORT
  CISCO_PHONE_AUTO_SMARTPORT
  CISCO_ROUTER_AUTO_SMARTPORT
  CISCO_SWITCH_AUTO_SMARTPORT
LINE    <cr>
Switch(config)# macro auto execute RADIUS_MAB_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=10
Switch(config)# exit
Switch# show shell triggers
User defined triggers
---------------------
Trigger Id: RADIUS_MAB_EVENT
Trigger description: MAC_AuthBypass Event
Trigger environment:
Trigger mapping function: CISCO_AP_SMARTPORT
```

```
<output truncated>
```

This example shows how to use the **show shell** *triggers* privileged EXEC command to view the event triggers in the switch software:

```
Switch# show shell triggers

User defined triggers
---------------------
Built-in triggers
-----------------
Trigger Id: CISCO_DMP_EVENT
Trigger description: Digital media-player device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1), The value
in the parenthesis is a default value
Trigger mapping function: CISCO_DMP_AUTO_SMARTPORT

Trigger Id: CISCO_IPVSC_EVENT
Trigger description: IP-camera device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1), The value
in parenthesis is a default value
Trigger mapping function: CISCO_IP_CAMERA_AUTO_SMARTPORT

Trigger Id: CISCO_PHONE_EVENT
Trigger description: IP-phone device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1) and
$VOICE_VLAN=(2), The value in the parenthesis is a default value
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT

Trigger Id: CISCO_ROUTER_EVENT
Trigger description: Router device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value
in the parenthesis is a default value
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_EVENT
Trigger description: Switch device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value
in the parenthesis is a default value
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_AP_EVENT
Trigger description: Autonomous ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value
in the parenthesis is a default value
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
Trigger description: Lightweight-ap device event to apply port configuration
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1),  The
value in the parenthesis is a default value
Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT
```

This example shows how to use the **show shell** *functions* privileged EXEC command to view the built-in macros in the switch software:

```
Switch# show shell functions
#User defined functions:

#Built-in functions:
function CISCO_AP_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface  $INTERFACE
```

```
                macro description $TRIGGER
                switchport trunk encapsulation dot1q
                switchport trunk native vlan $NATIVE_VLAN
                switchport trunk allowed vlan ALL
                switchport mode trunk
                switchport nonegotiate
                auto qos voip trust
                mls qos trust cos
            exit
        end
    fi
    if [[ $LINKUP -eq NO ]]; then
        conf t
            interface  $INTERFACE
                no macro description
                no switchport nonegotiate
                no switchport trunk native vlan $NATIVE_VLAN
                no switchport trunk allowed vlan ALL
                no auto qos voip trust
                no mls qos trust cos
                if [[ $AUTH_ENABLED -eq NO ]]; then
                    no switchport mode
                    no switchport trunk encapsulation
                fi
            exit
        end
    fi
}

function CISCO_SWITCH_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface  $INTERFACE
                macro description $TRIGGER
                auto qos voip trust
                switchport trunk encapsulation dot1q
                switchport trunk native vlan $NATIVE_VLAN
                switchport trunk allowed vlan ALL
                switchport mode trunk
            exit
        end
    else
         conf t
             interface  $INTERFACE
                 no macro description
                 no auto qos voip trust
                 no switchport mode trunk
                 no switchport trunk encapsulation dot1q
                 no switchport trunk native vlan $NATIVE_VLAN
                 no switchport trunk allowed vlan ALL
             exit
         end
    fi
}

<output truncated>
```

Configuring Auto Smartports User-Defined Macros

The Cisco IOS shell provides basic scripting capabilities for configuring the user-defined Auto Smartports macros. These macros can contain multiple lines and can include any CLI command. You can also define variable substitution, conditionals, functions, and triggers within the macro. This procedure is optional.

Beginning in privileged EXEC mode, follow these steps to map a user-defined event trigger to a user-defined macro.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto execute** *event trigger* [*parameter=value*] {*function contents*}	Specify a user-defined macro that maps to an event trigger. {*function contents*} Specify a user-defined macro to associate with the trigger. Enter the macro contents within braces. Begin the Cisco IOS shell commands with the left brace and end the command grouping with the right brace. (Optional) *parameter=value*—Replace default values that begin with $, enter new values in the form of name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...].
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to map a user-defined event trigger called media player to a user-defined macro.

a. Connect the media player to an 802.1x- or MAB-enabled switch port.

b. On the RADIUS server, set the attribute-value pair to **auto-smart-port** =MP_EVENT.

c. On the switch, create the event trigger MP_EVENT, and enter the user-defined macro commands shown below.

d. The switch recognizes the attribute-value pair=MP_EVENT response from the RADIUS server and applies the macro associated with this event trigger.

```
Switch(config)# shell trigger MP_EVENT mediaplayer
Switch(config)# macro auto execute MP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
 interface $INTERFACE
   macro description $TRIGGER
   switchport access vlan 1
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security violation restrict
   switchport port-security aging time 2
   switchport port-security aging type inactivity
   spanning-tree portfast
   spanning-tree bpduguard enable
   exit
fi
if [[ $LINKUP -eq NO ]]; then
```

```
conf t
interface $INTERFACE
     no macro description $TRIGGER
     no switchport access vlan 1
     if [[ $AUTH_ENABLED -eq NO ]]; then
        no switchport mode access
     fi
     no switchport port-security
     no switchport port-security maximum 1
     no switchport port-security violation restrict
     no switchport port-security aging time 2
     no switchport port-security aging type inactivity
     no spanning-tree portfast
     no spanning-tree bpduguard enable
     exit
fi
}
Switch(config)# end
```

Table 13-2 Supported Cisco IOS Shell Keywords

Command	Description
{	Begin the command grouping.
}	End the command grouping.
[[	Use as a conditional construct.
]]	Use as a conditional construct.
else	Use as a conditional construct.
-eq	Use as a conditional construct.
fi	Use as a conditional construct.
if	Use as a conditional construct.
then	Use as a conditional construct.
-z	Use as a conditional construct.
$	Variables that begin with the $ character are replaced with a parameter value.
#	Use the # character to enter comment text.

Table 13-3 Unsupported Cisco IOS Shell Reserved Keywords

Command	Description
|	Pipeline.
case	Conditional construct.
esac	Conditional construct.
for	Looping construct.
function	Shell function.
in	Conditional construct.
select	Conditional construct.
time	Pipeline.

Table 13-3 Unsupported Cisco IOS Shell Reserved Keywords (continued)

Command	Description
until	Looping construct.
while	Looping construct.

Configuring Static Smartports Macros

- Default Static Smartports Configuration, page 13-17
- Static Smartports Configuration Guidelines, page 13-17
- Applying Static Smartports Macros, page 13-18

Default Static Smartports Configuration

There are no static Smartports macros enabled on the switch.

Table 13-4 Default Static Smartports Macros

Macro Name[1]	Description
cisco-global	Use this global configuration macro to enable rapid PVST+, loop guard, and dynamic port error recovery for link state failures.
cisco-desktop	Use this interface configuration macro for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port.
cisco-phone	Use this interface configuration macro when connecting a desktop device such as a PC with a Cisco IP Phone to a switch port. This macro is an extension of the **cisco-desktop** macro and provides the same security and resiliency features, but with the addition of dedicated voice VLANs to ensure proper treatment of delay-sensitive voice traffic.
cisco-switch	Use this interface configuration macro when connecting an access switch and a distribution switch or between access switches connected by using small form-factor pluggable (SFP) modules.
cisco-router	Use this interface configuration macro when connecting the switch and a WAN router.
cisco-wireless	Use this interface configuration macro when connecting the switch and a wireless access point.

1. Cisco-default Smartports macros vary, depending on the software version running on your switch.

Static Smartports Configuration Guidelines

- When a macro is applied globally to a switch or to a switch interface, all existing configuration on the interface is retained. This is helpful when applying an incremental configuration.
- If a command fails because of a syntax or a configuration error, the macro continues to apply the remaining commands. You can use the **macro global trace** *macro-name* global configuration command or the **macro trace** *macro-name* interface configuration command to apply and debug a macro to find any syntax or configuration errors.
- Some CLI commands are specific to certain interface types. If you apply a macro to an interface that does not accept the configuration, the macro fails the syntax or the configuration check, and the switch returns an error message.

- Applying a macro to an interface range is the same as applying a macro to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.
- When you apply a macro to a switch or a switch interface, the macro name is automatically added to the switch or interface. You can display the applied commands and macro names by using the **show running-config** user EXEC command.

Applying Static Smartports Macros

Beginning in privileged EXEC mode, follow these steps to apply a static Smartports macro:

	Command	Purpose
Step 1	**show parser macro**	Display the Cisco-default static Smartports macros embedded in the switch software.
Step 2	**show parser macro name** *macro-name*	Display the specific macro that you want to apply.
Step 3	**configure terminal**	Enter global configuration mode.
Step 4	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	Apply each individual command defined in the macro to the switch by entering **macro global apply** *macro-name*. Specify **macro global trace** *macro-name* to apply and to debug a macro to find any syntax or configuration errors. Append the macro with the required values by using the **parameter** *value* keywords. Keywords that begin with **$** require a unique parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values for the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied. (Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. The corresponding value replaces all matching occurrences of the keyword.
Step 5	**interface** *interface-id*	(Optional) Enter interface configuration mode, and specify the interface on which to apply the macro.
Step 6	**default interface** *interface-id*	(Optional) Clear all configuration from the specified interface.
Step 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	Apply each individual command defined in the macro to the port by entering **macro global apply** *macro-name*. Specify **macro global trace** *macro-name* to apply and to debug a macro to find any syntax or configuration errors. Append the macro with the required values by using the **parameter** *value* keywords. Keywords that begin with **$** require a unique parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values for the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied. (Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. The corresponding value replaces all matching occurrences of the keyword.

	Command	Purpose
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show running-config interface** *interface-id*	Verify that the macro is applied to an interface.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

You can only delete a global macro-applied configuration on a switch by entering the **no** version of each command in the macro. You can delete a macro-applied configuration on a port by entering the **default interface** *interface-id* interface configuration command.

This example shows how to display the **cisco-desktop** macro, to apply the macro and to set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro cisco-desktop
------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

Displaying Auto Smartports and Static Smartports Macros

To display the Auto Smartports and static Smartports macros, use one or more of the privileged EXEC commands in Table 13-5.

Table 13-5 Commands for Displaying Auto Smartports and Static Smartports Macros

Command	Purpose
show macro auto	Displays information about Auto Smartports macros.
show parser macro	Displays all static Smartports macros.
show parser macro name *macro-name*	Displays a specific static Smartports macro.
show parser macro brief	Displays the static Smartports macro names.
show parser macro description [**interface** *interface-id*]	Displays the static Smartports macro description for all interfaces or for a specified interface.
show shell	Displays information about Auto Smartports event triggers and macros.