CHAPTER 12

Configuring Auto Smartports Macros

This chapter describes how to configure and apply Auto Smartports and static Smartports macros on the Catalyst 3560 switch.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

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.

In addition to Auto Smartports macros, 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.

Auto Smartports uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device invokes a CDP event trigger: Cisco IP phone, Cisco wireless access point, Cisco switch, or Cisco router. Other event triggers use MAC authentication bypass (MAB) and 802.1x authentication messages.

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 scripting capability, which is a BASH-like language syntax for command automation and variable replacement.

Configuring Auto Smartports

Default Auto Smartports Configuration

- Auto Smartports is disabled.
- Cisco IOS shell is enabled.

Table 12-1 shows the Auto Smartports built-in macros that are embedded in the switch software.

Table 12-1 Auto Smartports Built-in Macros

Macro Name	Description
CISCO_PHONE_AUTO_ SMARTPORT	Use this macro to apply the IP phone macro for Cisco IP phones. It enables QoS, port security, Address Resolution Protocol inspection (dynamic ARP inspection), IP source guard, DHCP snooping, storm control and spanning-tree protection on the port.
CISCO_SWITCH_AUTO_ SMARTPORT	Use this macro to apply the switch macro for Cisco switches. It enables trunking on the port.
CISCO_ROUTER_AUTO_ SMARTPORT	Use this macro to apply the router macro for Cisco routers. It enables QoS, trunking, and spanning-tree protection on the port.
CISCO_AP_AUTO_ SMARTPORT	Use this macro to apply the wireless access point (AP) macro for Cisco APs. It enables support for an autonomous wireless access point and QoS on the port.
CISCO_LWAP_AUTO_ SMARTPORT	Use this macro to apply the light-weight wireless access point macro for Cisco light-weight wireless APs. It enables QoS, port security, dynamic ARP inspection, IP source guard, DHCP snooping, storm control, and spanning-tree protection on the port.
CISCO_DOT1X_DESKTOP_ AUTO_SMARTPORT	Use this macro to apply the desktop macro for IEEE 802.1x-authenticated devices. It enables basic desktop configuration, including security and spanning-tree protection.
CISCO_DOT1X_EASY_AUTO _SMARTPORT	Use this macro to apply the desktop macro for IEEE 802.1x-authenticated desktop devices. It provides 802.1x, MAB, guest-VLAN, authentication-fail-VLAN support and reduces the 802.1x timeout to 3 seconds.
CISCO_DOT1X_MAB_ GUEST_AUTO_SMARTPORT	Use this macro to apply the desktop macro for 802.1x-, MAB-, and guest-VLAN-authenticated devices.
CISCO_DOT1X_MAB_ TIMEOUT_AUTO_ SMARTPORT	Use this macro to apply the desktop macro for 802.1x-, MAB-, and guest-VLAN-authenticated devices configured with an aggressive timeout.
CISCO_DOT1X_AUTH_ FAIL_AUTO_SMARTPORT	Use this macro to apply the desktop macro for 802.1x-, MAB-, and authentication-fail-VLAN-authenticated devices.
CISCO_DOT1X_CRITICAL_ AUTO_SMARTPORT	Use this macro to apply the desktop macro for 802.1x-, MAB-, and critical-VLAN-authenticated devices.

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.
- To avoid system conflicts when Auto Smartports macros are applied, remove all port configuration except for 802.1x authentication.
- If the macro conflicts with the original configuration, some macro commands might not be applied, or some antimacro commands might not be removed. (The antimacro is the portion of the applied macro that removes it at link down.)

  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 should not be a member of an EtherChannel when applying Auto Smartports macros.
- The built-in macro default data VLAN is VLAN 1. The default voice VLAN is VLAN 2. You should modify the built-in macro default values if your switch uses different VLANs. To view all built-in macro default values, use the **show shell** *functions* privileged EXEC command.
- 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, we recommend that you disable Auto Smartports on the port.
- If authentication is enabled on a port, the switch ignores CDP unless the **cdp-fallback** keyword is in the **macro auto global processing** global configuration command.
- The order of CLI commands within the macro and the corresponding antimacro can be different.

Enabling Auto Smartports

To configure the switch to automatically apply Auto Smartports macros on all ports, use the **macro auto global processing** global configuration command. To disable Auto Smartports macros on a specific port, use the **no auto global processing** in the interface mode.

Beginning in privileged EXEC mode, follow these steps.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro auto global processing** [**cdp-fallback**]	Globally enable Auto Smartports on the switch. (Optional) Use the **cdp-fallback** keyword to enable the switch to use CDP capability information when a port is 802.1x-enabled and the RADIUS server does not send an event trigger.
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 shell** *functions* and the **show shell** *triggers* privileged EXEC command to display the event triggers, the built-in macros, and the built-in macro default values.

This example shows how 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 Built-in Macros

The switch automatically maps from event triggers to built-in macros. You can replace the built-in macro default values with values that are specific to your switch.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command	Purpose
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_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*: • CISCO_PHONE_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1) and $VOICE_VLAN=(2). • CISCO_SWITCH_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=(1). • CISCO_ROUTER_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=(1). • CISCO_AP_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=(1). • CISCO_LWAP_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_DESKTOP_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_EASY_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_MAB_GUEST_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_MAB_TIMEOUT_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_AUTH_FAIL_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=(1). • CISCO_DOT1X_CRITICAL_AUTO_SMARTPORT (Optional) Specify the parameter values: $CRITICAL_VLAN=(1). (Optional) *parameter*=*value*—Replace default values that begin with **$**. Enter new values in the form of name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...]. Default values are shown in parenthesis.
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 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 Gi1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 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
```

Configuring 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.

Beginning in privileged EXEC mode, follow these steps to configure an event trigger.

	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_DOT1X_MAB_GUEST_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_DOT1X_MAB_GUEST_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_DOT1X_DESKTOP_AUTO_SMARTPORT
  CISCO_DOT1X_EASY_AUTO_SMARTPORT
  CISCO_DOT1X_MAB_GUEST_AUTO_SMARTPORT
  CISCO_DOT1X_MAB_TIMEOUT_AUTO_SMARTPORT
  CISCO_DOT1X_AUTH_FAIL_AUTO_SMARTPORT
  CISCO_DOT1X_CRITICAL_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_DOT1X_MAB_GUEST_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_DOT1X_MAB_GUEST_AUTO_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_PHONE_EVENT
Trigger description: Event for ip-phone macro
Trigger environment: ACCESS_VLAN=1 VOICE_VLAN=2
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_ROUTER_EVENT
Trigger description: Event for router macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_EVENT
Trigger description: Event for switch macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_AP_EVENT
Trigger description: Event for Wireless Access Point macro
Trigger environment: NATIVE_VLAN=1
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
Trigger description: Event for Wireless Lightweight Access Point macro
Trigger environment: NATIVE_VLAN=1
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.

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 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 Cisco Digital Media Player (DMP) to a user-defined macro.

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

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

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

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

```
Switch(config)# shell trigger CISCO_DMP_EVENT Cisco DMP player
Switch(config)# macro auto execute CISCO_DMP_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 12-2 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.

Table 12-2 Supported Cisco IOS Shell Keywords (continued)

Command	Description
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 12-3 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.
until	Looping construct.
while	Looping construct.

Configuring Static Smartports Macros

This section describes how to configure and enable static Smartports macros.

Default Static Smartports Configuration

There are no static Smartports macros enabled on the switch.

Table 12-4 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.

	Command	Purpose
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.
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 12-5.

Table 12-5 Commands for Displaying Auto Smartports and Static Smartports Macros

Command	Purpose
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.