CHAPTER 1

Auto Smartports and Static Smartports Macros

Auto 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 macro. When there is a link-down event, the switch removes the macro. For example, when you connect a Cisco IP phone to a port, Auto Smartports 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 port macros.

You can also manually configure and apply global macros.

The macros embedded in the switch software are groups of CLI commands.

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.

For information, see Chapter 2, “Configuring Auto Smartports and Static Smartports Macros.”

Static Smartports Macros

Static Smartports macros provide port configurations that you apply manually based on the device connected to the port. When you apply a static macro, the macro CLI commands 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.

Event Triggers

Auto Smartports uses event triggers to map macros to the source port of the event. The most common triggers are based on Cisco Discovery Protocol (CDP) messages received from another device. A CDP event trigger occurs when these devices are detected:

- Cisco switch
- Cisco router
- Cisco IP Phone
- Cisco Wireless Access Points, including autonomous and lightweight access points
- Cisco IP video surveillance camera
- Cisco digital media player

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 used to discover neighbor devices. These type, length, and value attributes and descriptions are referred to as TLVs. LLDP-supported devices use TLVs to receive and send information. This protocol advertises details such as device configuration information, capabilities, and identity. Auto Smartports uses the LLDP *system capabilities* TLV as the event trigger. Use the event trigger control feature to specify if the switch applies a macro based on the detection method, device type, or configured trigger.

For more information about configuring the LLDP system capabilities TLV attributes for Auto Smartports, see the “Configuring LLDP, LLDP-MED, and Wired Location Service” chapter in the switch-specific software configuration guides.

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 that has the desired configuration.

Beginning with Cisco IOS Release 15.0(1)SE, Auto Smartports can detect devices based on Dynamic Host Control Protocol (DHCP) options. There are predefined and customizable macros for devices detected through DHCP options.

User-Defined Files

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

Macro Persistence

The macro persistence feature causes macro configurations to remain enabled on the switch ports regardless of a link-down event. This eliminates multiple system log and configuration change notifications when the switch has link-up and link-down events or is a domain member or an end point in an EnergyWise network.

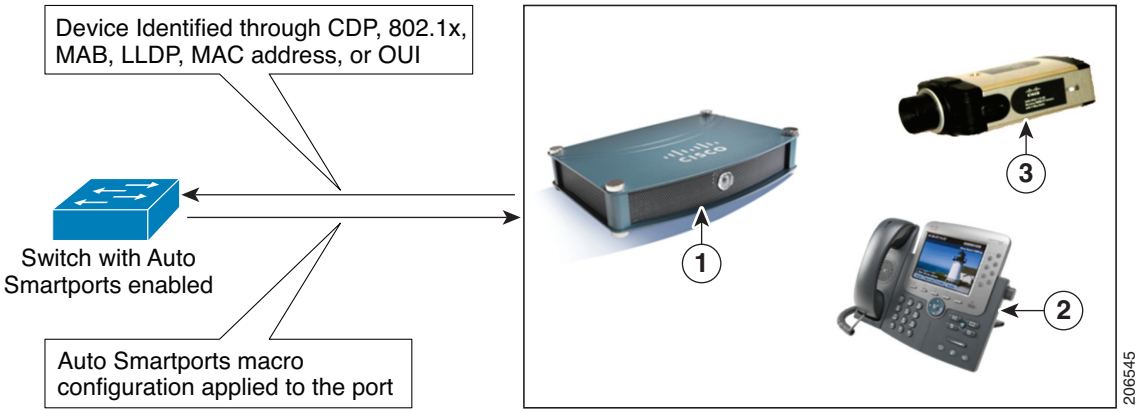
Managing Macros

You can use the Cisco LAN management system (LMS) tools to deploy macros to switches. When you define a custom macro, you must also configure and associate a trigger for it. For information on configuring user-defined triggers, see the "Configuring User-Defined Triggers for User-Defined Macros" section on page 2-22.

Auto Smartports and Cisco Medianet

Cisco Medianet enables intelligent services in the network infrastructure for a variety of video applications. A service of Medianet is autoprovisioning 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 1-1). The switch applies the applicable macro to enable the appropriate VLAN, standard quality of service (QoS), and auto-QoS settings for the device. The switch also uses a built-in MAC address group to detect the legacy Cisco digital media player (DMP), based on an OUI of of4400 or 23ac00. You can also create custom user-defined macros for any video device.

Figure 1-1 Cisco Medianet Deployment Example



1	Wireless access point	**3**	Cisco IP video surveillance camera
2	Cisco IP phone		

Device Classifier

Beginning with Cisco IOS Release 15.0(1) SE, the device classifier (DC) feature is enabled by default on the switch.

The DC collects information from MAC-OUI and protocols such as CDP, LLDP, and DHCP to identify devices. You must enable CDP and LLDP on the switch. To make DHCP options information available to the DC, you must enable the DHCP snooping feature on the switch. The device attributes collected from these protocols are evaluated against a set of profiles available to the DC to find the best match. The best-matched profile is used for device identification.

Device-classifier uses profile definitions—built-in and default profiles. The built-in profiles contain the device profiles that are known to the Auto Smartports module, comprising a limited set of Cisco devices. They are built into Cisco IOS and cannot be changed. The default profiles are stored as a text file in nonvolatile storage and allow the DC to identify a much larger set of devices. The default profiles are updated as part of the Cisco IOS archive download.

When a new device is detected, the corresponding shell trigger executes the Auto Smartports configuration macro. Auto Smartports has built-in mappings for a large set of devices. You can use the commands described in the "Configuring User-Defined Triggers for User-Defined Macros" section on page 2-22 to create new mappings. You can create the trigger mappings based on the profile name or device name that is provided by the DC.

For switch stacks, the DC runs only on the stack master. All the attributes for devices connected to stack master and stack member switch ports are available to the DC on the stack master. The device classification results are available only on the stack master. During a stack master failover event, the new stack master reclassifies all the devices. The device attributes for the existing and any new devices are available to the DC on the new stack master.

Device Visibility Mode

The DC function is enabled on the switch by default. You can disable it by using the **no macro auto monitor** global configuration command. The DC feature provides **show** commands to display the devices that are connected to the switch. It also provides information about the physical port to which the device is connected, along with device MAC address and other vendor information. Only directly connected devices, such as another Layer 2 switch, are classified on nonaccess ports. On access ports that are connected to hubs, device classification is limited to 32 devices.

When you enable Auto Smartports, the DC is automatically enabled.