Cisco Networking Capabilities 2.1 for Medianet

Configuration Guide

November 1, 2010

Contents

About This Guide

This guide describes how to configure, maintain, and troubleshoot Cisco® Networking Capabilities 2.1 for medianet.

Installation of Cisco switches, routers, and endpoint devices is beyond the scope of this document.

Audience

This guide is for network system administrators deploying and maintaining medianet capabilities. It assumes the following:

- You have a thorough understanding of data, voice, and video networking terminology and concepts.
- You have the required knowledge and skills to configure maintain and troubleshoot Cisco routers and switches.

Autoconfiguration and Location Information Overview

Autoconfiguration is one of the Cisco Networking Capabilities 2.1 for medianet. Autoconfiguration automates device configuration and registration to simplify management, movement, additions, and changes of equipment

Autoconfiguration has three components.

- The first component allows an endpoint device to announce and identify itself to the network. Typical endpoint devices use the Cisco Discovery Protocol or MAC address to announce themselves.
- The second component is the auto-smartport feature implemented in the access switch images of Cisco IOS® Software. This component applies device-specific configuration and quality-of-service (QoS) macros to switch ports upon detection of a media endpoint. The switch software comes with a set of built-in best-practice configuration macros for a variety of media endpoints.
- The third component is the set up and transmission of location information. Cisco IOS Software allows network operators to configure device-specific location information on the switches. This location information is then propagated to the endpoint devices.

Figure 1 shows the autoconfiguration solution and its components. Endpoint devices announce themselves through the Cisco Discovery Protocol or MAC address. The auto-smartport feature in the access switch applies device-specific configuration macros to the connecting port.

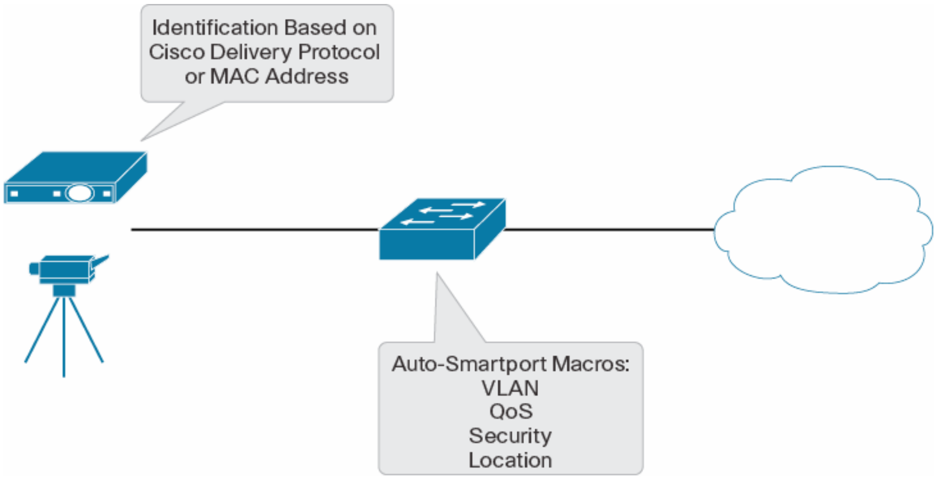
Identification Based on Cisco Delivery Protocol or MAC Address
Auto-Smartport Macros:
VLAN
QoS
Security
Location

Figure 1. Autoconfiguration Solution

Autoconfiguration Requirements

For more information about the requirements for using the autoconfiguration capability, please refer to the Cisco Networking Capabilities for Medianet data sheet.

Autoconfiguration Sample Topology and Configuration

Figure 2 shows an example of a typical Cisco medianet deployment.

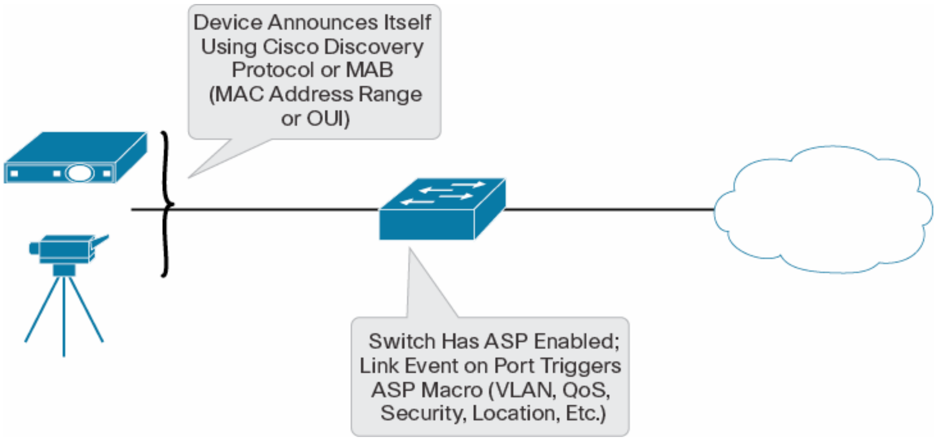
Device Announces Itself Using Cisco Discovery Protocol or MAB (MAC Address Range or OUI)
Switch Has ASP Enabled; Link Event on Port Triggers ASP Macro (VLAN, QoS, Security, Location, Etc.)

Figure 2. Typical Cisco Medianet Deployment

How to Deploy Autoconfiguration

Design Considerations for Enabling Auto-Smartports

A medianet device announces or identifies itself to the switch when it is connected in two ways:

- If the device supports Cisco Discovery Protocol, then first thing it does after the physical layer come up is to send a Cisco Discovery Protocol packet identifying itself (product ID, capabilities, etc.).
- All other devices can be identified based on their MAC addresses; this process is tied to the MAC address learning process. To use this method of identifying devices, you need to configure the MAC authentication bypass (MAB) mechanism on the switch. Please refer to Configure Auto-Smartports with MAB later in this document.

After a device has been identified by one of these mechanisms. The auto-smartport feature on the switch triggers an event associated with the detection of the device. This event applies the appropriate configuration macro associated with the trigger.

Steps for Configuring Auto-Smartports

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 a link-down event occurs on the port (the device is disconnected or powered down), the switch removes the macro.

The steps for configuring auto-smartports are:

- Enable auto-smartports macros (required).
- Configure auto-smartports at the port level (optional).
- Configure auto-smartports parameter values (optional).
- Configure MAC address groups (optional).
- Configure auto-smartports with MAB (optional).

Enable Auto-Smartport Macros

Auto-smartports can be enabled globally on the switch. You can turn off auto-smartports on an individual port by using the **no macro auto processing** command.

Beginning in privileged EXEC mode, follow the required procedure shown in Table 1.

Table 1. Steps for Enabling Auto-Smartports on a Switch

	Command	Purpose
Step 1	**configure terminal**	Changes to global configuration mode
Step 2	**macro auto global processing**	Globally enables macros on the switch
Step 3	**End**	Returns to privileged EXEC mode
Step 4	**show running-config**	Verifies that auto-smartports is enabled
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file

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

Configure Auto-Smartports at the Port Level

In some situations, it may be desirable not to have to the auto-smartports feature turned on for some ports because they may have special configurations on them: for example, a port connecting to an uplink switch or router, or ports configured as EtherChannels . On such ports, auto-smartports must be turned off.

This example shows how to enable macros on the switch and then how to disable macros on a specific interface:

```
CA3-SWITCH(config)#macro auto global processing
CA3-SWITCH(config)#int gi 1/0/13
CA3-SWITCH(config-if)#no macro auto processing
```

Configure Auto-Smartports Parameter Values

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

To change the default VLAN using macro parameters, you need to create a new VLAN on the switch.

Beginning in privileged EXEC mode, follow the steps shown in Table 2.

Table 2. Steps for Configuring Auto-Smartports Parameter Values

	Command	Purpose
Step 1	**show macro auto device**	Displays the macro default parameter values
Step 2	**configure terminal**	global configuration mode
Step 3	**vlan** *vlan-id*	(Optional) Lets you create or modify a VLAN: Enter a VLAN ID and switch to config-vlan mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.
Step 4	**name** *vlan-name*	(Optional) Lets you name a VLAN: Enter a name for the VLAN. If no name is entered for the VLAN, by default the word “VLAN” and leading zeros are appended to the vlan-id value. For example, VLAN0004 is the default VLAN name for VLAN 4.
Step 5	**Exit**	Returns to configuration mode
Step 6	**macro auto device {access-point | ip-camera | lightweight-ap | media-player | phone | router | switch***} [parameter=value]*	Replaces the specified macro default parameter values: Enter new values in the form of a name-value pair separated by spaces: *[<name1>=<value1> <name2>=<value2>...].* You can enter the VLAN ID or the VLAN name when specifying VLAN parameter values. Default values for each macro parameter are: • 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 7	**End**	Returns to privileged EXEC mode
Step 8	**show macro auto device**	Verifies your entries
Step 9	**copy running-config startup-config**	(Optional) Saves 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.

Configure MAC Address Groups

For devices such as printers or third-party security cameras that do not support neighbor discovery protocols such as Cisco Discovery Protocol, use the MAC address–based trigger configurations. This optional procedure requires these steps:

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

Existing digital media players (DMPs) and devices that do not support Cisco Discovery Protocol should be configured using a MAC address–based trigger for autoconfiguration.

Beginning in privileged EXEC mode, follow the steps shown in Table 3.

Table 3. Steps for Configuring MAC Address Groups

	Command	Purpose
Step 1	**configure terminal**	Changes to global configuration mode
Step 2	**macro auto mac-address-group** *name*	Specifies the group name and changes to MAC address configuration mode
Step 3	**[mac-address list** *list*] **| [oui [list** *list* **| range** *start-value* **size** *number***]]**	Configures a list of MAC addresses separated by spaces: 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 format separated by spaces. • **range:** Enter the starting OUI hexadecimal value (start-value). • **size:** Enter the length of the range (number) from 1 to 5 to create a list of sequential addresses.
Step 4	**exit**	Returns to configuration mode
Step 5	**macro auto execute** ***address_trigger*** **built-in** ***macro name***	Maps the MAC address group trigger to a built-in or user-defined macro*: The MAC address trigger is applied to an interface after 65 seconds. The switch uses this hold time to apply a Cisco Discovery Protocol event trigger instead of the MAC address trigger.
Step 6	**end**	Returns to privileged EXEC mode
Step 7	**show macro auto address-group**	Verifies your entries
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file

* For more information about user-defined macros, please refer to the Cisco Auto-Smartports Configuration Guide.

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 that maps to a macro defined by the **macro auto execute** global configuration command. Entering **no macro auto execute mac-address-group** removes only 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:

This example shows how to create a MAC address group event trigger called *address_trigger for third party IP cameras* and how to verify it:

```
Switch(config)# macro auto mac-address-group 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)# macro auto execute ADDRESS_TRIGGER builtin macro
Switch(config)# macro auto execute mac-address-trigger builtin
CISCO_IP_CAMERA_AUTO_SMARTPORT
Switch(config)# end

Switch# show running configuration | include macro
macro auto mac-address-group ADDRESS_TRIGGER
mac auto execute mac-address-trigger builtin
CISCO_IP_CAMERA_AUTO_SMARTPORT
 macro description CISCO_IP_CAMERA_EVENT
!
<output truncated>
```

The example shows how to create an OUI list with five sequential addresses starting with 00000A and how to verify your entries:

```
Switch(config)# macro auto mac-address-group size5ouilist
Switch(config-addr-grp-mac)# oui range 00000A size 5
Switch(config-addr-grp-mac)# exit
Switch(config)# mac auto execute size5-ouilist builtin macro
Switch(config)# macro auto execute mac-address-trigger builtin
CISCO_IP_CAMERA_AUTO_SMARTPORT
Switch(config)# end
```

Configure Auto-Smartports with MAB

For devices that do not support neighbor discovery protocols such as Cisco Discovery Protocol and IEEE 802.1x authentication, the switch can be configured with MAB. It is assumed that RADIUS server and dot1x authentication is already configured on the switch. When using MAB or IEEE 802.1x authentication as an event trigger, create a 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, follow the steps shown in Table 4.

Table 4. Steps for Configuring Auto-Smartports with MAB

	Command	Purpose
Step 1	**Configure terminal**	Changes to global configuration mode
Step 2	**shell trigger** *identifier description*	Specifies the event trigger identifier and description: The identifier should have no spaces or hyphens between words.
Step 3	macro auto execute *address_trigger* built-in *macro name*	Maps the MAC address group trigger to a built-in or user-defined macro*: The MAC address trigger is applied to an interface after 65 seconds. The switch uses this hold time to apply a Cisco Discovery Protocol or Link Layer Discovery Protocol (LLDP) event trigger instead of the MAC address trigger.
Step 4	**Interface** *interface-id*	Specifies the port that is connected to a medianet endpoint device and changes to interface configuration mode
Step 5	**Mab**	Enables MAC address–based authentication on a port
Step 6	**End**	Returns to privileged EXEC mode
Step 7	**Show sell triggers**	Displays the event triggers on the switch
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file

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

This example shows how to map a user-defined event trigger called RADIUS_MAB_EVENT generated by a third-party IP camera to the built-in macro CISCO_CAMERA_AUTO_SMARTPORT and replace the default ACCESS VLAN with VLAN 101.

1. On the RADIUS server, set the attribute-value pair to:

```
auto-smart-port=RADIUS_MAB_EVENT
```

2. Create a user-defined trigger and map a system-defined macro to it.

   a. Create the trigger event:

```
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
```

   b. Map a system defined macro to the trigger event:

```
Switch(config)# macro auto execute RADIUS_MAB_EVENT builtin macro auto
execute RADIUS_MAB_EVENT builtin CISCO_CAMERA_AUTO_SMARTPORT
ACCESS_VLAN=101
```

3. Enable MAB and dot1x on the interface:

```
Switch(config)# interface GigabitEthernet1/5
Switch(config-interface)# mab
Switch(config-interface)# authentication port-control auto
Switch(config-interface)# dot1x pae authenticator
```

4. Enable authentication, authorization, and accounting (AAA) and RADIUS on the switch:

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)# radius-server host 10.10.10.1
Switch(config)#radius-server key cisco123
Switch(config)#radius-server vsa send authentication
```

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

Troubleshooting Tips

Troubleshooting Autoconfiguration Failure for a Newly Added Device with Port-Security Configuration

The switch remembers the MAC address of the previous device connected to a port with the **port-security sticky** configuration. A newly added endpoint will fail port security if a previously learned MAC address with a sticky configuration exists.

To disable sticky learning on an interface, use the **no switchport port-security mac-address sticky** interface configuration command. The interface converts the sticky secure MAC addresses to dynamic secure addresses. However, if you have previously saved the configuration with the sticky MAC addresses, you should save the configuration again after entering the no **switchport port-security mac-address sticky** command, or the sticky addresses will be restored if the switch reboots.

Use the **clear port-security {all | configured | dynamic | sticky}** privileged EXEC mode command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

To delete a specific secure MAC address from the address table, use the **no switchport port-security mac-address** *mac-address* interface configuration command. To delete all dynamic secure addresses on an interface from the address table, enter the **no switchport port-security** interface configuration command followed by the **switchport port-security** command (to reenable port security on the interface). If you use the **no switchport port-security mac-address sticky** interface configuration command to convert sticky secure MAC addresses to dynamic secure MAC addresses before entering the **no switchport port-security** command, all secure addresses on the interface except those that were manually configured are deleted.

You must specifically delete configured secure MAC addresses from the address table by using the **no switchport port-security mac-address** *mac-address* interface configuration command.

Verifying Cisco Discovery Protocol

Making sure Cisco Discovery Protocol is enabled on the interface when the end device is being detected using Cisco Discovery Protocol:

```
SWITCH#sh cdp neighbors gi1/5 detail
-------------------------
Device ID: SEP1C17D34191EA
Entry address(es):
Platform: Cisco IP Phone 9971,  Capabilities: Host Phone Two-port Mac
Relay
Interface: GigabitEthernet1/5,  Port ID (outgoing port): Port 1
Holdtime : 145 sec
Second Port Status: Down

Version :
sip9971.9-0-0-77

advertisement version: 2
Duplex: full
```

```
Power drawn: 11.700 Watts
Power request id: 60058, Power management id: 1
Power request levels are:11700 0 0 0 0
Management address(es):
```

Cisco Discovery Protocol can be enabled using the following commands at the global level and at the interface level:

```
Configure terminal
cdp run
interface GigabitEthernet1/0/1
cdp enable
```

The following debug messages are displayed by debug cdp events and debug cdp packets command:

```
Sep 21 15:50:40.896: CDP-EV: Packet Received from MGMT-SW-FF1424 with
capability = 28 and Platform string = cisco WS-C3560-24TS on interface
GigabitEthernet1/0/1
Sep 21 15:50:47.002: CDP-PA: Packet received from 8843E1397DA6 on
interface GigabitEthernet1/0/3
Sep 21 15:50:47.002: **Entry  found in cache**
Sep 21 15:50:47.011: CDP-EV: Packet Received from 8843E1397DA6 with
capability = 10 and Platform string = CIVS-IPC-2500 on interface
GigabitEthernet1/0/3
Sep 21 15:50:49.091: CDP-PA: Packet received from C-EDGE-SW-MOD on
interface GigabitEthernet1/0/9
Sep 21 15:50:49.091: **Entry  found in cache**
Sep 21 15:50:49.091: CDP-EV: Packet Received from C-EDGE-SW-MOD with
capability = 29 and Platform string = cisco SM-ES3G-16-P on interface
GigabitEthernet1/0/9
```

Verifying Shell Functions

To verify the list of commands generated for a macro, use the following commands:

```
Mediant-switch#sh shell functions CISCO_DMP_AUTO_SMARTPORT

function CISCO_DMP_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface  $INTERFACE
                macro description $TRIGGER
                switchport access vlan $ACCESS_VLAN
                switchport mode access
                switchport block unicast
                mls qos trust dscp
                spanning-tree portfast
                switchport port-security
                switchport port-security maximum 1
                switchport port-security violation shutdown
                spanning-tree bpduguard enable
                priority-queue out
            exit
        end
    fi
    if [[ $LINKUP -eq NO ]]; then
        conf t
            interface  $INTERFACE
                no macro description
                no switchport access vlan $ACCESS_VLAN
                no switchport block unicast
                no switchport port-security
                no switchport port-security maximum 1
                no switchport port-security violation shutdown
                no mls qos trust dscp
                no spanning-tree portfast
                no spanning-tree bpduguard enable
                no priority-queue out
                if [[ $AUTH_ENABLED -eq NO ]]; then
                    no switchport mode access
                fi
            exit
        end
    fi
}
```

You can use the following command to see all macro definitions currently active:

```
Mediant-switch#sh shell functions
```

Debugging MAB

If MAB fails, you can use the following command to identify the cause of the problem:

- **show radius server-group all:** Shows the definition and status of the server
- **show radius statistics:** Displays statistics information for packets exchanged

The following example shows RADIUS debugging output for a successful MAB authentication. The main parameters are highlighted.

```
Switch#
.Aug  4 19:30:00.499 EDT: %SYS-5-CONFIG_I: Configured from console by
console
.Aug  4 19:30:26.675 EDT: %DOT1X-5-FAIL: Authentication failed for
client (Unknown MAC) on Interface Gi1/5 AuditSessionID
0A1C150200000007004E6707
.Aug  4 19:30:26.675 EDT: %AUTHMGR-7-RESULT: Authentication result
'no-response' from 'dot1x' for client (Unknown MAC) on Interface Gi1/5
AuditSessionID 0A1C150200000007004E6707
.Aug  4 19:30:26.675 EDT: %AUTHMGR-7-FAILOVER: Failing over from
'dot1x' for client (Unknown MAC) on Interface Gi1/5 AuditSessionID
0A1C150200000007004E6707
.Aug  4 19:30:33.700 EDT: %AUTHMGR-5-START: Starting 'mab' for client
(1c17.d341.91ea) on Interface Gi1/5 AuditSessionID
0A1C150200000007004E6707
.Aug  4 19:30:33.700 EDT: RADIUS/ENCODE(0000000C):Orig. component type
= DOT1X
.Aug  4 19:30:33.700 EDT: RADIUS(0000000C): Config NAS IP: 0.0.0.0
```

```
.Aug  4 19:30:33.700 EDT: RADIUS/ENCODE(0000000C): acct_session_id: 11

.Aug  4 19:30:33.700 EDT: RADIUS(0000000C): sending

.Aug  4 19:30:33.700 EDT: RADIUS/ENCODE: Best Local IP-Address
10.28.21.2 for Radius-Server 10.29.18.103

.Aug  4 19:30:33.700 EDT: RADIUS(0000000C): Send Access-Request to
10.29.18.103:1812 id 1645/3, len 209

.Aug  4 19:30:33.700 EDT: RADIUS:  authenticator 11 E3 54 71 E3 B2 2B
1C - 61 C8 E9 8A 71 F1 59 C3

.Aug  4 19:30:33.700 EDT: RADIUS:  User-Name           [1]   14
"1c17d34191ea"

.Aug  4 19:30:33.700 EDT: RADIUS:  User-Password       [2]   18  *

.Aug  4 19:30:33.700 EDT: RADIUS:  Service-Type        [6]   6   Call
Check                [10]

.Aug  4 19:30:33.700 EDT: RADIUS:  Framed-MTU          [12]  6   1500

.Aug  4 19:30:33.700 EDT: RADIUS:  Called-Station-Id   [30]  19  "00-
15-C6-AA-54-D4"

.Aug  4 19:30:33.700 EDT: RADIUS:  Calling-Station-Id  [31]  19  "1C-
17-D3-41-91-EA"

.Aug  4 19:30:33.700 EDT: RADIUS:  Message-Authenticato[80]  18

.Aug  4 19:30:33.700 EDT: RADIUS:   D9 CD 7C 9D B9 F1 BE 2D 3C F6 B6
B9 E0 18 41 44             [ |-<AD]

.Aug  4 19:30:33.700 EDT: RADIUS:  EAP-Key-Name        [102] 2   *

.Aug  4 19:30:33.700 EDT: RADIUS:  Vendor, Cisco       [26]  49

.Aug  4 19:30:33.700 EDT: RADIUS:   Cisco AVpair       [1]   43
"audit-session-id=0A1C150200000007004E6707"

.Aug  4 19:30:33.700 EDT: RADIUS:  NAS-Port-Type       [61]  6
Ethernet                  [15]

.Aug  4 19:30:33.700 EDT: RADIUS:  NAS-Port            [5]   6   50105

.Aug  4 19:30:33.700 EDT: RADIUS:  NAS-Port-Id         [87]  20
"GigabitEthernet1/5"

.Aug  4 19:30:33.700 EDT: RADIUS:  NAS-IP-Address      [4]   6
10.28.21.2

.Aug  4 19:30:33.720 EDT: RADIUS: Received from id 1645/3
10.29.18.103:1812, Access-Accept, len 60

.Aug  4 19:30:33.720 EDT: RADIUS:  authenticator 33 24 0F 61 99 B2 CF
40 - 43 FE 3A 11 35 41 98 0E

.Aug  4 19:30:33.720 EDT: RADIUS:  Vendor, Cisco       [26]  40

.Aug  4 19:30:33.720 EDT: RADIUS:   Cisco AVpair       [1]   34
"auto-smart-port=RADIUS_MAB_EVENT"

.Aug  4 19:30:33.720 EDT: RADIUS(0000000C): Received from id 1645/3

.Aug  4 19:30:33.720 EDT: RADIUS/DECODE: Ignoring unknown attribute
from protocol type RADIUS

.Aug  4 19:30:33.720 EDT: %MAB-5-SUCCESS: Authentication successful
for client (1c17.d341.91ea) on Interface Gi1/5 AuditSessionID
0A1C150200000007004E6707

.Aug  4 19:30:33.720 EDT: %AUTHMGR-7-RESULT: Authentication result
'success' from 'mab' for client (1c17.d341.91ea) on Interface Gi1/5
AuditSessionID 0A1C150200000007004E6707

.Aug  4 19:30:34.770 EDT: %AUTHMGR-5-SUCCESS: Authorization succeeded
for client (1c17.d341.91ea) on Interface Gi1/5 AuditSessionID
0A1C150200000007004E6707

.Aug  4 19:30:34.770 EDT: RADIUS/ENCODE(0000000C):Orig. component type
= DOT1X

.
```

Showing Triggers and Macros

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_CUSTOM_EVENT
Trigger description: Custom macroevent to apply user defined
configuration
Trigger environment: User can define the macro
Trigger mapping function: CISCO_CUSTOM_AUTOSMARTPORT

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
…
…
<Truncated CLI output>
```

Tips

Identifying MAC Addresses

You need to identify MAC address information from the endpoints to configure the Cisco Secure Access Control System (ACS) and Dynamic Host Configuration Protocol (DHCP). The easiest way to identify the MAC address after the endpoint is connected to the switch is by using the following command:

```
show mac address-table interface <interface>
```

Configuring Location

Use the following commands to configure civic location information on the switch:

```
Switch#configure terminal
Switch(config)#location civic-location identifier 1
Switch(config-civic)# building 1
Switch(config-civic)#city RTP
Switch(config-civic)# floor 1
Switch(config-civic)# room LAB1
Switch(config)#interface GigabitEthernet1/0/13
Switch(config-int)# location civic-location-id 1
Switch(config-int)# location additional-location-information Camp1
```

For more information on configuring location, please refer to the Configuring Location TLV and Wired Location Service.

Displaying Default Auto-Smartport Macros

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 and the built-in macros.

The default built in macro functions and associated devices are:

- **CISCO_AP_AUTO_SMARTPORT**: Cisco wireless access point macro
- **CISCO_DMP_AUTO_SMARTPORT**: Cisco Digital Media Player (DMP) macro
- **CISCO_IPVSC_AUTO_SMARTPORT**: Cisco Video Surveillance IP Camera macro
- **CISCO_LWAP_AUTO_SMARTPORT**: Cisco Lightweight Access Point macro
- **CISCO_PHONE_AUTO_SMARTPORT**: Cisco IP Phone macro
- **CISCO_ROUTER_AUTO_SMARTPORT**: Cisco router macro
- **CISCO_SWITCH_AUTO_SMARTPORT**: Cisco switch macro

This example shows how to see the Cisco DMP macro parameter values and how to change the default voice ACCESS_VLAN to 20. When you change the default values, they are not immediately applied on the interfaces with existing applied macros. The configured values are applied at the next link event. Note that the exact text string was used for ACCESS_VLAN. The entry is case sensitive.

```
CA3-SWITCH# #sh macro auto device media-player
Device:media-player
Default Macro:CISCO_DMP_AUTO_SMARTPORT
Current Macro:CISCO_DMP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=1

CA3-SWITCH# config t
CA3-SWITCH(config)# macro auto device media-player ACCESS_VLAN=20
CA3-SWITCH(config)# shutdown
CA3-SWITCH(config)# no shutdown
CA3-SWITCH(config)# end

CA3-SWITCH# #sh macro auto device media-player
Device:media-player
Default Macro:CISCO_DMP_AUTO_SMARTPORT
Current Macro:CISCO_DMP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=20
```

The following example shows a macro triggered configuration for the Cisco IP Camera on a Cisco Catalyst 3750 Series Switch:

```
CA3-SWITCH#sh run int gi 1/0/3
Building configuration...

Current configuration : 383 bytes
!
interface GigabitEthernet1/0/3
 description TO IP-CAMERA
 switchport mode access
 switchport block unicast
 switchport port-security
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust device ip-camera
 mls qos trust dscp
 macro description CISCO_IPVSC_EVENT
 auto qos video ip-camera
spanning-tree portfast
 spanning-tree bpduguard enable
end
```

For More Information

For detailed, step-by-step configuration information, please see Cisco Auto-smartports Configuration Guide and Configuring Auto-QoS.

For design considerations, please refer to the section Auto-Smartports Configuration Guidelines in the document Configuring Auto-Smartport Macros.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C17-629409-01 11/10