Configuring Management Interfaces

This module lists the following topics:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points. The management interface has the only consistently “pingable” in-band interface IP address on the controller. You can access the GUI of the controller by entering the management interface IP address of the controller in the address field of your browser.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.

If the service port is in use, the management interface must be on a different supernet from the service-port interface.

Note To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator must ensure that only authorized clients gain access to the management network through proper CPU ACLs, or use a firewall between the client dynamic interface and the management network.

Caution Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.

Caution Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.

Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Authentication Type for Management Interfaces

For any type of management access to the controller, bet it SSH, Telnet, or HTTP, we recommend that you use any one authentication type, which can be TACACS+, RADIUS, or Local, and not a mix of these authentication types. Ensure that you take care of the following:

- Authentication type (TACACS+, RADIUS, or Local), must be the same for all management access and for all AAA authentication and authorization parameters.
- The method list must be explicitly specified in the HTTP authentication.

Example

Follow these steps to configure Telnet:

1. Configure TACACS+ server by entering these commands:
   a. **tacacs server** *server-name*
   b. **address ipv4** *ip-address*
   c. **key** *key-name*
2. Configure the server group name by entering these commands:
   a. **aaa group server tacacs+** *group-name*
   b. **server name** *name*
3. Configure authentication and authorization by entering these commands:
   a. **aaa authentication login** *method-list* **group** *server-group*

b **aaa authorization exec** *method-list* **group** *server-group*

Note These and all the other authentication and authorization parameters must be using the same database, be it RADIUS, TACACS+, or Local. For example, if command authorization has to be enabled, it also needs to be pointing to the same database.

4 Configure HTTP to use the above method lists:

1 **ip http authentication aaa login-auth** *method-list*
You must explicitly specify the method list, even if the method list is "default".

2 **ip http authentication aaa exec-auth** *method-list*

Note

- Do not configure any method-lists on the "line vty" configuration parameters. If the above steps and the line vty have different configurations, then line vty configurations take precedence.
- The database should be the same across all management configuration types such as SSH/Telnet and webui.
- You must explicitly define the method list for HTTP authentication.

Workaround

As a workaround, enter the following commands:

1 **aaa authentication login default group** *server-group* **local**
2 **aaa authorization exec default group** *server-group* **local**

Pre-requisites for Configuring Management Interfaces

The pre-requisites for configuring the management interfaces on the controller follow:

- For Cisco 5700 Series Controllers in a non-link-aggregation (non-LAG) configuration, the management interface must be on a different VLAN than any dynamic AP-manager interface. Otherwise, the management interface cannot fail over to the port that the AP-manager is on.
- If the service port is in use, the management interface must be on a different supernet from the service-port interface.
- To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator must ensure that only authorized clients gain access to the management network through proper CPU ACLs, or use a firewall between the client dynamic interface and the management network.

Restrictions for Configuring Management Interfaces

The following are the restrictions for configuring the controller's management interface:

- Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.
- Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Configuring the Management Interface using the CLI

Before You Begin

You must use the following steps to configure management interfaces on the controller. You can also use these steps to configure the AP manager interfaces on the controller. These general instructions apply to all management interfaces.

SUMMARY STEPS

1. **show ip interface brief**
2. **config terminal**
3. **wireless management interface vlan vlanID**
4. **end**
5. **show wireless interface summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip interface brief**	Displays all the interfaces in the controller.
Step 2	**config terminal**	Enters global configuration mode.
Step 3	**wireless management interface vlan vlanID**	Creates a management interface by providing the values for the VLAN (VLAN identifier).
Step 4	**end**	Returns to EXEC mode.
Step 5	**show wireless interface summary**	Displays all the wireless interfaces in the controller.

Configuring the Management Interface

This module contains the following topics:

Feature History and Information For Configuring Management Interfaces

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.