Configuring Wired Guest Access

Wired Guest Access

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract.

You can create a basic peer to peer WLAN ACL and apply it to the wired guest WLAN. This will not block peer to peer traffic and the guest users can still communicate with each other.

This section contains the following subsections:

Prerequisites for Configuring Wired Guest Access

To configure wired guest access on a wireless network, you must perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

Restrictions for Configuring Wired Guest Access

- Wired guest access interfaces must be tagged.
- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.
- The controller does not use the callStationIDType parameter configured for the Radius server while authenticating wired clients, instead the controller uses the system MAC address configured for the callStationIDType parameter.

Configuring Wired Guest Access (GUI)

Step 1 To create a dynamic interface for wired guest user access, choose **Controller** > **Interfaces**. The Interfaces page appears.

Step 2 Click **New** to open the **Interfaces > New** page.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Click **Apply** to commit your changes.

Step 5 In the **Port Number** text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

Step 6 Select the **Guest LAN** check box.

Step 7 Click **Apply** to commit your changes.

Step 8 To create a wired LAN for guest user access, choose **WLANs**.

Step 9 On the WLANs page, choose **Create New** from the drop-down list and click **Go**. The **WLANs** > **New page** appears.

Step 10 From the Type drop-down list, choose **Guest LAN**.

Step 11 In the **Profile Name** text box, enter a name that identifies the guest LAN. Do not use any spaces.

Step 12 From the WLAN ID drop-down list, choose the ID number for this guest LAN.

Note You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).

Step 13 Click **Apply** to commit your changes.

Step 14 Select the **Enabled** check box for the Status parameter.

Step 15 Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing *Step 16* and *Step 17*.

Step 16 From the Ingress Interface drop-down list, choose the VLAN that you created in *Step 3*. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 17 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18 If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security** > **Layer 3**. The **WLANs > Edit (Security > Layer 3)** page appears.

Step 19 From the Layer 3 Security drop-down list, choose one of the following:

- **None**—Layer 3 security is disabled.
- **Web Authentication**—Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
- **Web Passthrough**—Allows users to access the network without entering a username and password.

  Note There should not be a Layer 3 gateway on the guest wired VLAN, as this would bypass the web authentication done through the controller.

Step 20 If you choose the Web Passthrough option, an **Email Input** check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21 To override the global authentication configuration set on the Web Login page, select the **Override Global Config** check box.

Step 22 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wired guest users:

- **Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized**—Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 23 If you chose External as the web authentication type in *Step 22*, choose **Security > AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note You can configure the Authentication and LDAP Server using both IPv4 and IPv6 addresses.

Note The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 24 To establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

a. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.

b. Click **Up** and **Down** until the desired server type is at the top of the box.

c. Click the < arrow to move the server type to the priority box on the left.

d. Repeat these steps to assign priority to the other servers.

Step 25 Click **Apply**.

Step 26 Click **Save Configuration**.

Step 27 Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Step 1 Create a dynamic interface (VLAN) for wired guest user access by entering this command:

config interface create *interface_name vlan_id*

Step 2 If link aggregation trunk is not configured, enter this command to map a physical port to the interface:

config interface port *interface_name primary_port* {*secondary_port*}

Step 3 Enable or disable the guest LAN VLAN by entering this command:

config interface guest-lan *interface_name* {**enable | disable}**

This VLAN is later associated with the ingress interface created in *Step 5*.

Step 4 Create a wired LAN for wired client traffic and associate it to an interface by entering this command:

config guest-lan create *guest_lan_id interface_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).

Note To delete a wired guest LAN, enter the **config guest-lan delete** *guest_lan_id command.*

Step 5 Configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch by entering this command:

config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 Configure an egress interface to transmit wired guest traffic out of the controller by entering this command:

config guest-lan interface *guest_lan_id interface_name*

Note If the wired guest traffic is terminating on another controller, repeat *Step 4* and *Step 6* for the terminating (anchor) controller and *Step 1* through *Step 5* for the originating (foreign) controller. Additionally, configure the **config mobility group anchor add** {**guest-lan** *guest_lan_id* | **wlan** *wlan_id} IP_address* command for both controllers.

Step 7 Configure the security policy for the wired guest LAN by entering this command:

config guest-lan security {**web-auth enable guest_lan_id** | **web-passthrough enable** *guest_lan_id*}

Note Web authentication is the default setting.

Step 8 Enable or disable a wired guest LAN by entering this command:

config guest-lan {enable | disable} *guest_lan_id*

Step 9 If you want wired guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the guest LAN for which it should display:

- **config guest-lan custom-web login-page** *page_name guest_lan_id—Defines a web login page.*
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id—Defines a web login failure* page.

  Note To use the controller's default login failure page, enter the **config guest-lan custom-web loginfailure-page none** *guest_lan_id* command.

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*—Defines a web logout page.

  Note To use the controller's default logout page, enter the **config guest-lan custom-web logout-page none** *guest_lan_id* command.

Step 10 If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Step 11 If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 Define the web login page for wired guest users by entering this command:

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.

- **customized** displays the custom web pages (login, login failure, or logout) that were configured in *Step 9*.
- **external** redirects users to the URL that was configured in *Step 10*.

Step 13 Use a guest-LAN specific custom web configuration rather than a global custom web configuration by entering this command:

config guest-lan custom-web global disable *guest_lan_id*

Note If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

Step 14 Save your changes by entering this command:

save config

Note Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

Step 15 Display the customized web authentication settings for a specific guest LAN by entering this command:

show custom-web {all | guest-lan guest_lan_id}

Note If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Step 16 Display a summary of the local interfaces by entering this command:

show interface summary

Note The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

Display detailed interface information by entering this command:

show interface detailed *interface_name*

Step 17 Display the configuration of a specific wired guest LAN by entering this command:

show guest-lan *guest_lan_id*

Note Enter the **show guest-lan summary** command to see all wired guest LANs configured on the controller.

Step 18 Display the active wired guest LAN clients by entering this command:

show client summary guest-lan

Step 19 Display detailed information for a specific client by entering this command:

show client detail *client_mac*

Supporting IPv6 Client Guest Access

The client is in WebAuth Required state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once authenticated, the user's MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

In order to support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com which returns a DNSv6 (AAAA) record.