




Wireless Guest Access

Overview

There is an increasing requirement in organisations to provide Wi-Fi network access to contractors and visitors. This expanded network access enables higher productivity, improved collaboration, and better service; however, it necessitates that a guest access policy be established to address increased network usage and security issues.

By implementing a broad-based solution to guest access, an organisation can control network access, eliminate ad hoc IT support requirements, track guest network usage and securely separate guest traffic from internal resources.

The main technical requirements for a complete guest access solution are outlined below:

- Complete integration into the enterprise network and its resources
- Logical separation (segmentation) of guest traffic from corporate traffic
- Authentication and login capabilities

An existing enterprise wired and wireless network infrastructure can be used to implement a wireless guest network. No separate, overlay network is required to support guest access.

Therefore, the overall implementation and maintenance costs of a guest network are greatly reduced.

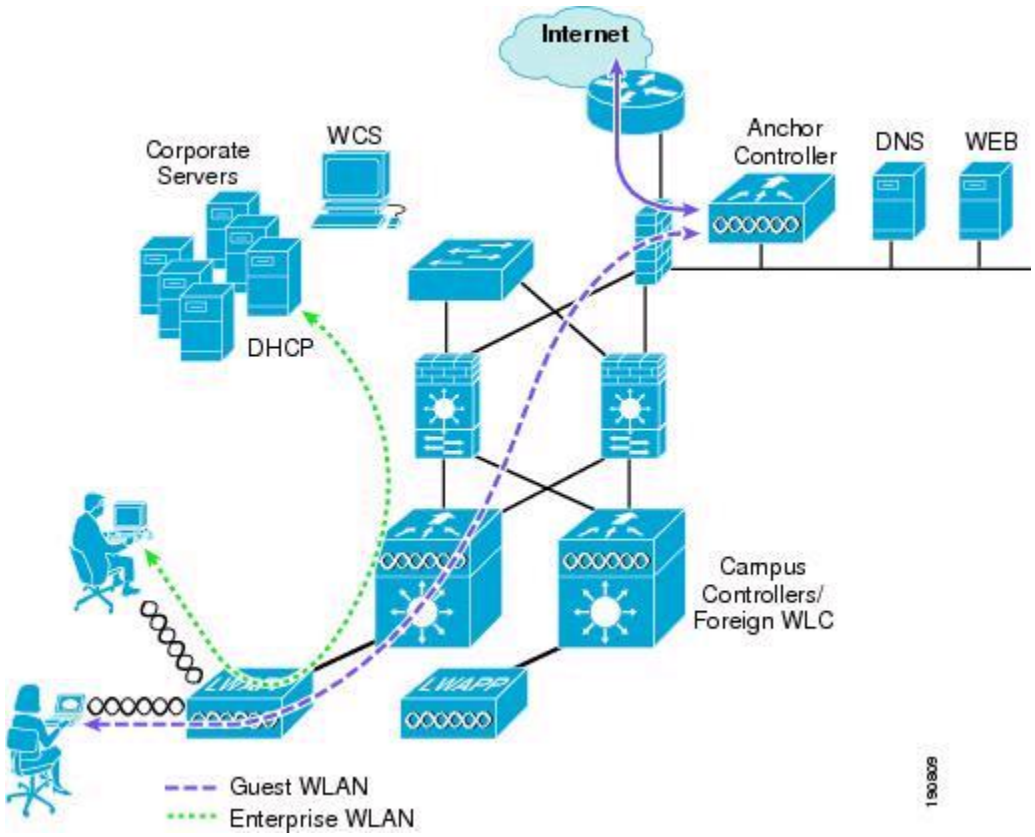
To successfully implement a guest network on an existing wired or wireless network, the following critical elements are required:

- A dedicated guest SSID/WLAN - Required within all wireless networks that require guest access.
- Guest traffic segregation or path isolation - To restrict guest user traffic to distinct, independent logical traffic paths within a shared physical network infrastructure.
- Access Control - To identify any user or device that logs onto the network for assignment to appropriate groups by employing an authentication process.
- Guest User Credential Management - To support creation of temporary credentials for a guest by an authorised user. This function may reside within an access control platform or a component of AAA or other management system.

Guest Access using the Cisco Unified Wireless Solution

The Cisco Unified WLAN solution offers a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the centralised architecture. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLC endpoints. The benefit of this approach is that there are no additional protocols or segmentation techniques that must be implemented to isolate guest traffic from the enterprise. See Figure 1 for an example of guest access topology using a centralised WLAN architecture.

Figure 1 Centralised Controller Guest Access



As shown in Figure 1, a WLC is located in the DMZ where it performs an "anchor" function. This anchor controller is responsible for terminating EoIP tunnels that originate from other campus WLCs throughout the network. These "foreign" controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Guest WLANs, instead of being switched locally

to a corresponding VLAN, are instead transported via an EoIP tunnel to the anchor controller. Specifically, guest WLAN data frames are encapsulated using CAPWAP from the AP to the foreign controller and then encapsulated in EoIP from the foreign WLC to a guest VLAN defined on the anchor WLC. In this way, guest user traffic is forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise network.

WLAN Controller Guest Access

The WLC Guest Access solution is self-contained and does not require any external platforms to perform access control, web portal, or AAA services. All these functions are configured and run within the anchor controller. However, the option exists to implement one or all of these functions externally and will be discussed later in the document.

Supported Platforms

The anchor function, which includes tunnel termination, web authentication, and access control, is supported on the following WLC platforms (using version 4.0 and later software images):

- Cisco 5508 Series
- Cisco 4400 Series
- Cisco 6500 Series (WISM)
- Cisco 3750 with integrated WLC

The following WLC platforms cannot be used for anchor functions, but can be used for standard controller deployments and guest mobility tunnel origination (foreign WLC) to a designated anchor controller(s):

- Cisco WLAN Controller Module for Integrated Service Routers (ISR)

- Cisco 2100/2500 Series WLC

Path Isolation and the Guest Anchor Controller

The guest anchor controller is usually located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN. An EoIP tunnel is established between the internal WLAN controllers and the guest anchor controller in order to ensure path isolation of guest traffic from enterprise data traffic. Path isolation is a critical security management feature for guest access. It ensures that security and quality of service (QoS) policies can be separate, and are differentiated between guest traffic and corporate or internal traffic.

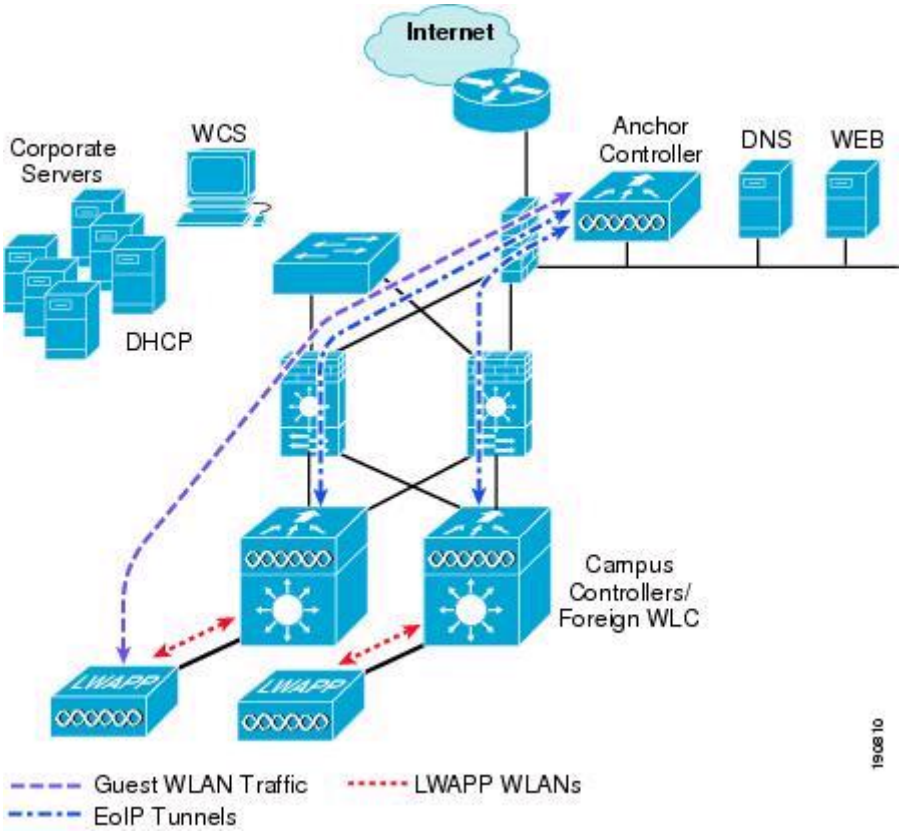
An important feature of the Cisco Unified Wireless Network architecture is the ability to use an EoIP tunnel to statically map one or more provisioned WLANs (that is, SSIDs) to a specific guest anchor controller within the network. All traffic—both to and from a mapped WLAN—traverses a static EoIP tunnel that is established between a remote controller and the guest anchor controller.

Using this technique, all associated guest traffic can be transported transparently across the enterprise network to a guest anchor controller that resides in the unsecured network area. (See Figure 2.)

The EoIP tunnel carries the guest traffic from the internal WLAN controller to the anchor controller in the clear. It is important to point out that the primary requirement for securely carrying guest traffic is path isolation. Security features such as confidentiality or integrity, delivered by the likes of IPsec are not required and offer little to no additional risk mitigation when compared to EoIP tunnels. If a guest user wishes to ensure confidentiality of their traffic, they will simply rely on solutions such as IPsec VPN clients or application level encryption in the form of SSL/TLS.

There are no known attacks against EoIP tunnels that would allow a guest user to ‘break-out’ and start attacking the internal infrastructure. Of course, mis-configuration of the WLAN estate could lead to compromise but this attack vector is not mitigated through technology, but through comprehensive and robust operating and change-control procedures.

Figure 2 Anchor Controller and EoIP Tunnels



Anchor Controller Positioning

Because the anchor controller is responsible for termination of guest WLAN traffic and subsequent access to the Internet, it is typically positioned in the Internet DMZ. In doing so, rules can be established within the firewall to precisely manage communications between authorised controllers throughout the enterprise and the anchor controller. Such rules might including filtering on source or destination controller addresses, UDP port 16666 for inter-WLC communication, and IP protocol ID 97 Ethernet in IP for client traffic. Other rules that might be needed include the following:

- TCP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80 or 443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for CLI access

DHCP Services

As previously described, guest traffic is transported at Layer 2 via EoIP. Therefore, the first point at which DHCP services can be implemented is either locally on the anchor controller or the controller can relay client DHCP requests to an external server.

Routing

Guest traffic egress occurs at the anchor controller. Guest WLANs are mapped to a dynamic interface/VLAN on the anchor. Depending on the topology, this interface might connect to an interface on a firewall, or directly to an Internet border router. Therefore, a client's default gateway IP is either that of the firewall or the address of a VLAN/interface on the first hop router. For ingress routing, it is assumed the guest VLAN is directly connected to a DMZ interface on a firewall or to an interface on a border router. In either case, the guest (VLAN) subnet is known as a directly connected network and advertised accordingly.

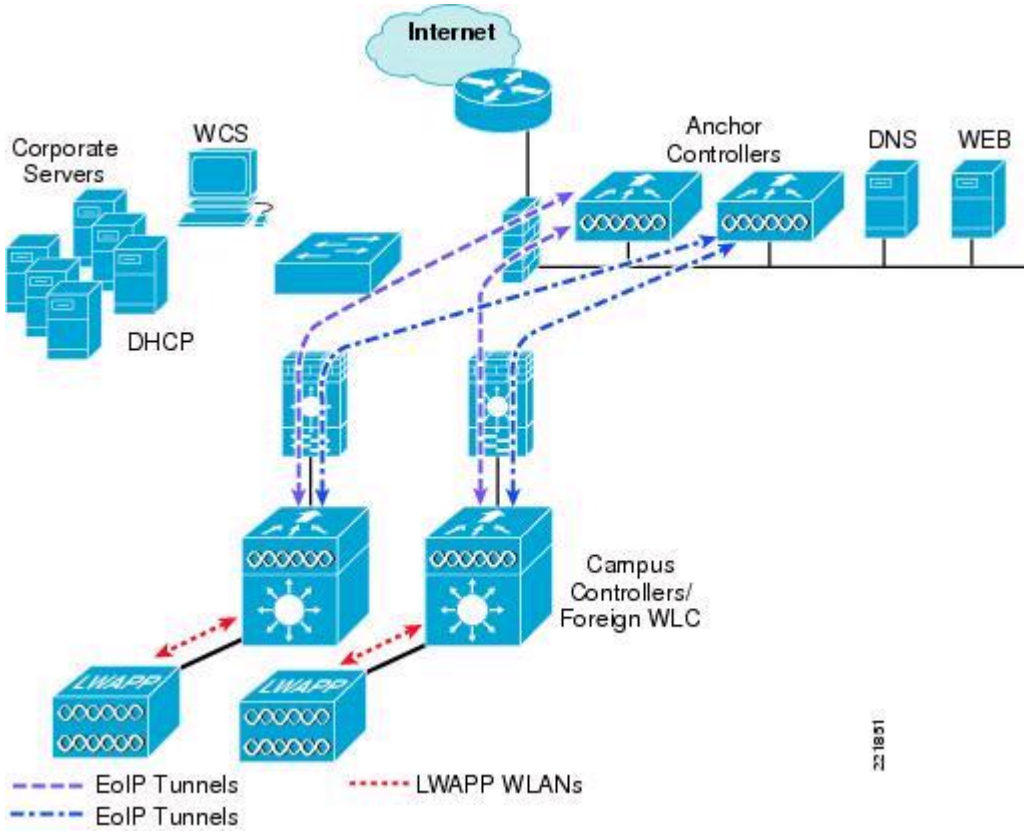
Anchor Controller Redundancy

Beginning with Release 4.1 of Unified Wireless solution software, a "guest N+1" redundancy capability was added to the auto anchor/mobility functionality. This new feature introduces an automatic ping function that enables a foreign controller to proactively ping anchor controllers to verity control and data path connectivity. In the event of failure or an active anchor becomes unreachable, the foreign controller does the following:

- Automatically detects that the anchor has become unreachable
- Automatically disassociates any wireless clients that were previously associated with the unreachable anchor
- Automatically re-associates wireless client(s) to an alternate anchor WLC

With guest N+1 redundancy, two or more anchor WLCs can be defined for a given guest WLAN. Figure 3 shows a generic guest access topology with anchor controller redundancy.

Figure 3 Guest Access Topology with Guest Anchor N+1 Redundancy



Keep in mind the following with regard to guest N+1 redundancy:

- A given foreign controller load balances wireless client connections across the list of anchor controllers configured for the guest WLAN. There is currently no method to designate one anchor as primary with one or more secondary anchors.

- Wireless clients that are associated with an anchor WLC that becomes unreachable are re-associated with another anchor defined for the WLAN. When this happens, assuming web authentication is being used, the client is redirected to the web portal authentication page and required to re-submit their credentials.

Web Portal Authentication

The Cisco Centralised Guest Access solution offers a built-in web portal that is used to solicit guest credentials for authentication and offers simple branding capabilities, along with the ability to display disclaimer or acceptable use policy.

The web portal page is available on all Cisco WLAN controller platforms and is invoked by default when a WLAN is configured for Layer 3 web policy-based authentication.

If a more customised page is required, administrators have the option of importing and locally storing a customised page. Additionally, if an organisation wants to use an external web server, the controller can be configured to redirect to this in place of using the internal server.

Guest Credentials Management

Guest credentials can be created and managed centrally using WCS beginning with release 4.0 and later. A network administrator can create a limited privilege account within WCS that permits lobby ambassador access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted to do is create and assign guest credentials to controllers that have web-policy configured WLANs.

As with many configuration tasks within WCS, guest credentials are created using templates. Beginning with release 4.1, the following new guest user template options and capabilities were introduced:

- There are two types of guest templates: one for scheduling immediate guest access with limited or unlimited lifetime, and the other permits administrators to schedule "future" guest access and offers time of day as well as day of week access restrictions.

- The solution offers administrators the ability to e-mail credentials to guest users. Additionally, when the "schedule" guest template is used, the system automatically e-mails credentials for each new day (interval) that access is offered.

- Guest credentials can be applied to the WLC(s) based on a (guest) WLAN SSID and WCS mapping information; campus/building/floor location or based on a WLAN SSID and a specific controller or list of controllers. The latter method is used when deploying guest access using the guest mobility anchor method as discussed in this document.

Guest credentials, once applied, are stored locally on the (anchor) WLC (under Security > Local Net Users) and remain there until expiration of the "Lifetime" variable as defined in the guest template. If a wireless guest is associated and active when their credentials expire, the WLC stops forwarding traffic and returns to the WEBAUTH_REQD policy state for that user. Unless the guest credentials are re-applied (to the controller), the user is no longer able to access the network.

Guest User Authentication

As previously discussed in Guest Credentials Management, when an administrator uses WCS or a local account on a controller to create guest user credentials, those credentials are stored locally on the controller, which in the case of a centralised guest access topology, would be the anchor controller.

When a wireless guest logs in through the web portal, the controller handles the authentication in the following order:

1. The controller checks its local database for username and password and, if present, grants access.

If no user credentials are found, then:

2. The controller checks to see if an external RADIUS server has been configured for the guest WLAN. If so, then the controller creates a RADIUS access-request packet with the user name and password and forwards it to the selected RADIUS server for authentication.

If no specific RADIUS servers have been configured for the guest WLAN:

3. The controller checks its global RADIUS server configuration settings. Any external RADIUS servers configured with the option to authenticate "network" users are queried with the guest user credentials. Otherwise, if no RADIUS servers have "network user" checked, and the user has not authenticated as a result of 1 or 2 above, authentication fails.

External Authentication

WLC and WCS guest account management (lobby ambassador) capabilities can be used only to create and apply guest user credentials for local authentication on the WLC. However, there may be cases where an enterprise already has an existing guest management /authentication solution deployed as part of a wired guest access or NAC solution. If this is the case, the anchor controller/guest WLAN can be configured to forward web portal authentication to an external RADIUS server, as described in Guest User Authentication.

The default protocol used by the controller to authenticate web users is Password Authentication Protocol (PAP). In the event you are authenticating web users to an external AAA server, be sure to verify the protocols supported by that server. The anchor controller can also be configured to use CHAP or MD5-CHAP for web authentication.

Guest Pass-through

Another variation of wireless guest access is to bypass user authentication altogether and allow open access. However, an organisation may still need to present an acceptable use policy or disclaimer page to users before granting access. If this is the case, then a guest WLAN can be configured for web policy pass through. In this scenario, a guest user is redirected to a portal page containing disclaimer information. Pass through mode also has an option for a user to enter an e-mail address before.

Important Notice

"The guidance provided in this document is of a generic nature and cannot be specific to your organisation or operations. Please contact your Cisco partner or Account Manager to discuss your specific requirements. The guidance is provided in good faith based upon reference materials sourced from organisations up to the date of publication. Errors and omissions are accepted. No warranty is given or implied."

