# Preguntas Más Frecuentes sobre Acceso Guest Inalámbrico

## Contenido

# Introducción

En este documento se describe la información de las preguntas más frecuentes (FAQ) sobre la función de acceso inalámbrico de invitado, que forma parte de la red inalámbrica unificada de Cisco.

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

# ¿Qué es un túnel Ethernet sobre IP (EoIP) al área de red no segura?

Cisco recomienda el uso de un controlador dedicado al tráfico de invitados. Este controlador se conoce como el controlador de anclaje de invitado.

El controlador de anclaje de invitado suele encontrarse en un área de red no segura, a menudo denominada zona desmilitarizada (DMZ). Otros controladores de WLAN internos desde donde se origina el tráfico se encuentran en la LAN empresarial. Se establece un túnel EoIP entre los controladores WLAN internos y el controlador de anclaje de invitado para garantizar el aislamiento de la ruta del tráfico de invitados del tráfico de datos de la empresa. El aislamiento de rutas es una función de administración de seguridad fundamental para el acceso de invitados. Garantiza que las políticas de seguridad y calidad del servicio (QoS) pueden ser independientes y diferenciarse entre el tráfico de invitados y el tráfico interno o corporativo.

Una función importante de la arquitectura Cisco Unified Wireless Network es la capacidad de utilizar un túnel EoIP para asignar estáticamente una o más WLAN (es decir, SSID) a un controlador de anclaje de invitado específico dentro de la red. Todo el tráfico, tanto hacia como desde una WLAN asignada, atraviesa un túnel EoIP estático que se establece entre un controlador remoto y el controlador de anclaje de invitado.

Con esta técnica, todo el tráfico de invitados asociado se puede transportar de forma transparente a través de la red de la empresa a un controlador de anclaje de invitado que reside en el área de red no segura.

# ¿Cómo selecciono el controlador adecuado para implementar como controlador de anclaje de invitado?

La selección del controlador de anclaje de invitado es una función de la cantidad de tráfico de

invitado según lo definido por el número de sesiones de cliente invitado activas, o según lo definido por la capacidad de la interfaz de enlace ascendente en el controlador, o ambos.

El rendimiento total y las limitaciones del cliente por controlador de anclaje de invitado son los siguientes:

- Controlador de LAN inalámbrica Cisco 2504: 4 interfaces de 1 Gbps * y 1000 clientes invitados
- Cisco 5508 Wireless LAN Controller (WLC): 8 Gbps y 7000 clientes invitados
- Módulo de servicios inalámbricos Cisco Catalyst serie 6500 (WiSM-2): 20 Gbps y 15 000 clientes
- Controlador de LAN inalámbrica (WLC) Cisco 8500: 10 Gbps y 64 000 clientes

---

Nota: Los Cisco 7500 WLC no se pueden configurar como controlador de anclaje de invitado. Consulte ¿Qué controladores se pueden utilizar para soportar el acceso de invitado en el área de red no segura? para la lista de WLCs que soportan la función de anclaje de invitado.

---

Se puede almacenar un máximo de 2048 nombres de usuario y contraseñas de invitado en la base de datos de cada controlador. Por lo tanto, si el número total de credenciales de invitado activas supera este número, se necesita más de un controlador. Como alternativa, las credenciales de invitado se pueden almacenar en un servidor RADIUS externo.

El número de puntos de acceso en la red no afecta a la selección del controlador de anclaje de invitado.

## ¿Cuántos túneles Ethernet sobre IP (EoIP) se pueden terminar en un controlador de anclaje de invitado?

Un controlador de anclaje de invitado puede terminar hasta 71 túneles EoIP desde controladores WLAN internos. Esta capacidad es la misma en cualquier modelo del controlador de LAN inalámbrica de Cisco excepto WLC- 2504. El controlador 2504 puede terminar hasta 15 túneles EoIP. Se puede configurar más de un controlador de anclaje de invitado si se requieren túneles adicionales.

Los túneles EoIP se cuentan por controlador WLAN, independientemente del número de WLAN tunelizadas o identificadores de conjunto seguro (SSID) en cada EoIP.

Se configura un túnel EoIP entre el controlador de anclaje de invitado y cada controlador interno que admite puntos de acceso con asociaciones de clientes invitados.

## ¿Puedo crear túneles Ethernet sobre IP (EoIP) entre

## controladores que ejecutan diferentes versiones de software?

No todas las versiones de software del controlador de LAN inalámbrica lo admiten. En tales casos, el control remoto y el controlador de anclaje deben ejecutar la misma versión del software WLC. Sin embargo, las versiones recientes del software permiten que los controladores de anclaje y remotos tengan versiones diferentes.

Esta matriz enumera las versiones del software Wireless LAN Controller con las que puede crear los túneles EoIP.

**EoIP Tunnel Combination Between WLC Versions**

| Anchor / Remote | 4.1.185 | 4.2.X | 5.0.X | 5.1.X | 5.2.X | 6.0.X | 7.0.X |
|---|---|---|---|---|---|---|---|
| 4.1.185 | ✓ | | | | | | |
| 4.2.X | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| 5.0.X | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5.1.X | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 6.0.X | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 7.0.X | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

4.2.x = 4.2.61.0, 4.2.99.0, 4.2.112.0, 4.2.130.0, 4.2.173.0, 4.2.176.0, 4.2.205.0, 4.2.207.0, 4.2.209.0
5.0.x = 5.0.148.0, 5.0.148.2
5.1.x = 5.1.151.0, 5.1.163.0
5.2.x = 5.2.157.0, 5.2.178.0, 5.2.193.0
6.0.X = 6.0.182.0, 6.0.188.0, 6.0.196.0, 6.0.199.0, 6.0.199.4
7.0.X = 7.0.98.0, 7.0.116.0 , 7.0.220.0

## ¿Se puede utilizar el controlador de LAN inalámbrica de Cisco serie 2100/2500 como controlador de anclaje de invitado en el área de red no segura?

Sí, a partir de la versión 7.4 del software Cisco Unified Wireless Network, el controlador de LAN inalámbrica de Cisco serie 2500 puede terminar (hasta 15 túneles EoIP) el tráfico de invitados fuera del firewall. El controlador de LAN inalámbrica de Cisco serie 2000 solo puede originar túneles de invitado.

## ¿Se puede utilizar el módulo de controlador de LAN inalámbrica de Cisco para routers de servicios integrados (WLCM o WLCM2) como controlador de anclaje de invitado en el área de red no segura?

No, el WLCM o el WLCM2 no pueden terminar los túneles de invitado. El WLCM sólo puede originar túneles de invitado.

## ¿Qué controladores se pueden utilizar para admitir el acceso de invitados en el área de red no segura?

La función de anclaje de túnel de invitado, que incluye terminación de túnel EoIP, autenticación Web y control de acceso de clientes invitados, es compatible con estas plataformas de controlador de LAN inalámbrica de Cisco con imágenes de software de la versión 4.0 o posterior:

- Módulo de servicios inalámbricos Cisco Catalyst serie 6500 (WiSM2)
- Controlador de LAN inalámbrica de la serie Cisco WiSM-2
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Controlador de LAN inalámbrica de la serie 5508 de Cisco
- Cisco 2500 Series Wireless LAN Controller (compatibilidad introducida en la versión de software 7.4)

## Si se utiliza un controlador de anclaje de invitado fuera del firewall, ¿qué puertos de firewall están abiertos para que los invitados puedan acceder al trabajo?

En cualquier firewall entre el controlador de anclaje de invitado y los controladores remotos, estos puertos deben estar abiertos:

- Movilidad heredada: protocolo IP 97 para el tráfico de datos de usuario, puerto UDP 16666
- Nueva movilidad: puertos UDP 16666 y 16667

Para la administración opcional, estos puertos de firewall deben estar abiertos:

- SSH/Telnet - Puerto TCP 22/23
- TFTP: puerto UDP 69
- NTP: puerto UDP 123

- SNMP - Puertos UDP 161 (obtención y establecimiento) y 162 (desvíos)
- HTTPS/HTTP: puerto TCP 443/80
- Syslog: puerto TCP 514
- Puerto UDP 1812 y 1813 de cuenta/autenticación RADIUS

## ¿Puede el tráfico de invitados pasar a través de un firewall con la traducción de direcciones de red (NAT) configurada?

Se debe utilizar NAT uno a uno en el túnel EoIP que atraviesa un firewall.

## En un escenario WLC externo de anclaje, ¿qué WLC envía la contabilización RADIUS?

En este escenario, la autenticación es siempre hecha por el WLC de anclaje. Por lo tanto, la contabilización RADIUS es enviada por el WLC de anclaje.

---

Nota: en una implementación de Autenticación web central (CWA) y/o Cambio de autorización (CoA), la contabilidad RADIUS debe estar DESACTIVADA en el delimitador y utilizarse únicamente en el WLC externo.

---

## El túnel de invitado entre el controlador interno y el controlador de anclaje falla. Veo estos registros en el WLC: `mm_listen.c:5373 MM-3-INVALID_PKT_RECVD: Recibió un paquete no válido de 10. 40.220.18. Miembro de origen:0.0.0.0. miembro de origen desconocido..` ¿Por qué?

Usted verifica el estado del túnel desde la GUI del WLC en la página WLANs. Haga clic en el cuadro desplegable junto a una WLAN y elija Anclas de movilidad, que contiene el estado del control y la ruta de datos. El mensaje de error se ve debido a una de estas razones:

1. Los controladores internos y de anclaje se encuentran en versiones de código diferentes. Asegúrese de que ejecutan las mismas versiones del código.
2. Configuraciones erróneas en la configuración de anclaje de movilidad. Compruebe que la DMZ se configura como el ancla de movilidad y que los WLC internos tienen el WLC de la DMZ configurado como el ancla de movilidad. Para obtener más información sobre cómo configurar el ancla de movilidad, refiérase a la sección Configuración de la Movilidad de Anclaje Automático de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0. Esto provocaría que los usuarios invitados no pudieran pasar el tráfico.

## En una configuración de acceso de invitado inalámbrico, los clientes no reciben la dirección IP del servidor DHCP. El mensaje de error Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP drop REPLY from Export-Foreign STA aparece en el controlador interno. ¿Por qué?

En una configuración de acceso de invitado inalámbrico, la configuración del proxy DHCP en los controladores de anclaje de invitado y el controlador interno deben coincidir. De lo contrario, la solicitud DHCP de los clientes se descarta y aparece este mensaje de error en el controlador interno:

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

Utilice este comando para cambiar la configuración del proxy dhcp en el WLC:

<#root>

```
(Cisco Controller) >
```

**config dhcp proxy ?**

```
enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

Utilice el comando show dhcp proxy en ambos controladores para verificar que ambos controladores tengan la misma configuración de proxy DHCP.

<#root>

```
(Cisco Controller) >
```

**show dhcp proxy**

```
DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

## Si el tráfico de invitados se tuneliza al área de red no segura, ¿dónde obtienen los clientes invitados una dirección IP?

El tráfico de invitados se transporta dentro de la empresa en la capa 3 mediante EoIP. Por lo tanto, el primer punto en el que se pueden implementar servicios de protocolo de configuración dinámica de host (DHCP) es localmente en el controlador de anclaje de invitado, o el controlador de anclaje de invitado puede retransmitir las solicitudes DHCP del cliente a un servidor externo. Éste es también el método por el que se controla la resolución de direcciones del Sistema de nombres de dominio (DNS).

## ¿El controlador de LAN inalámbrica de Cisco admite portales web para la autenticación de invitados?

Cisco Wireless LAN Controllers, versión de software 3.2 o posterior, proporciona un portal web integrado que captura las credenciales de invitados para la autenticación y ofrece funciones de marca sencillas, además de la capacidad de mostrar la renuncia de responsabilidad y la información de la política de uso aceptable.

## ¿Cómo puedo personalizar el portal web?

Para obtener información sobre cómo personalizar un portal web, consulte Elección de la Página de Login de Autenticación Web.

## ¿Cómo se gestionan las credenciales de invitado?

Las credenciales de invitado se pueden crear y gestionar de forma centralizada mediante Cisco Wireless Control System (WCS) versión 7.0 o Network Control System (NCS) versión 1.0. Un administrador de red puede establecer una cuenta administrativa con privilegios limitados en WCS que permita el acceso de "embajador de recepción" con el fin de crear credenciales de invitado. En WCS o NCS, la persona con una cuenta de embajador de recepción puede crear, asignar, supervisar y eliminar credenciales de invitado para el controlador que actúa como controlador de anclaje de invitado.

El embajador del lobby puede ingresar el nombre de usuario (o ID de usuario) y la contraseña de invitado, o las credenciales pueden ser generadas automáticamente. También hay un parámetro de configuración global que permite el uso de un nombre de usuario y una contraseña para todos los invitados, o un nombre de usuario y una contraseña únicos para cada invitado.

Para configurar la cuenta de embajador de recepción en el WCS, refiérase a la sección Creación de Cuentas de Usuario Invitado de la Guía de Configuración de Cisco Wireless Control System, Versión 7.0.

## ¿Está disponible la función de embajador en el vestíbulo en el controlador de LAN inalámbrica de Cisco además del sistema de control inalámbrico (WCS) o NCS?

Yes. Si el WCS o NCS no está implementado, un administrador de red puede establecer una

cuenta de embajador de recepción en el controlador de anclaje de invitado. Una persona que inicia sesión en el controlador de anclaje de invitado mediante la cuenta de embajador de recepción solo tiene acceso a las funciones de administración de usuarios invitados.

Si hay varios controladores de anclaje de invitado, se debe utilizar un WCS o NCS para configurar simultáneamente nombres de usuario en varios controladores de anclaje de invitado.

Para obtener información sobre cómo crear cuentas de embajador de lobby usando Wireless LAN Controllers, refiérase a la sección Creación de una Cuenta de Embajador de Lobby de la Guía de Configuración de Cisco Wireless LAN Controller, Release 7.0.

## ¿Se pueden autenticar los invitados con un servidor de autenticación, autorización y contabilidad (AAA) externo?

Yes. Las solicitudes de autenticación de invitado se pueden retransmitir a un servidor RADIUS externo.

## ¿Qué ocurre cuando un invitado inicia sesión?

Cuando un invitado inalámbrico inicia sesión a través del portal web, el controlador de anclaje de invitado maneja la autenticación realizando estos pasos:

1. El controlador de anclaje de invitado verifica su base de datos local en busca de nombre de usuario y contraseña y, si están presentes, otorga acceso.
2. Si no hay credenciales de usuario presentes localmente en el controlador de anclaje de invitado, el controlador de anclaje de invitado verifica las configuraciones de WLAN para ver si se ha configurado un servidor o servidores RADIUS externos para el WLAN de invitado. Si es así, el controlador crea un paquete de solicitud de acceso RADIUS con el nombre de usuario y la contraseña y lo reenvía al servidor RADIUS seleccionado para la autenticación.
3. Si no se han configurado servidores RADIUS específicos para la WLAN, el controlador verifica sus valores de configuración globales del servidor RADIUS. Cualquier servidor RADIUS externo configurado con la opción de autenticar "usuario de red" se consulta con las credenciales del usuario invitado. De lo contrario, si ningún servidor tiene seleccionado "usuario de red" y el usuario no se ha autenticado en los pasos 1 ó 2, la autenticación fallará.

## ¿Es posible omitir la autenticación de usuario invitado y mostrar solo la opción de renuncia de responsabilidad de la página web?

Yes. Otra opción de configuración del acceso inalámbrico de invitado es omitir por completo la autenticación de usuario y permitir el acceso abierto. Sin embargo, es posible que sea necesario presentar una política de uso aceptable y una página de exención de responsabilidad a los invitados antes de conceder el acceso. Para ello, se puede configurar una WLAN de invitado para

el paso a través de la política web. En este escenario, un usuario invitado es redirigido a una página del portal web que contiene información de renuncia de responsabilidad. Para habilitar la identificación del usuario invitado, el modo de paso a través también tiene una opción para que un usuario ingrese una dirección de correo electrónico antes de conectarse.

## ¿Necesitamos tener el control remoto y el controlador de anclaje de invitado en el mismo grupo de movilidad?

No. El controlador de anclaje de invitado y el control remoto pueden estar en grupos de movilidad separados.

## Si hay más de un SSID de invitado, ¿se puede dirigir cada WLAN (SSID) a un portal de páginas web único?

Yes. Todo el tráfico de invitados, ya sea en una única WLAN o en varias, se redirige a una página web. A partir de la versión 4.2 o posterior del WLC, cada WLAN se puede dirigir a una página del portal web única. Consulte la sección Asignación de Páginas de Login, Login Failure y Logout por WLAN de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.

## ¿Cuál es la funcionalidad de la nueva configuración en la versión 7.0 del WLC, WebAuth en la falla del filtro de Mac?

Si una WLAN tiene configurada una seguridad de Capa 2 (mac-filter) y Capa 3 (webauth-on-macfilter-failure), el cliente pasa al estado RUN si se pasa cualquiera de las dos. Y si falla la seguridad de la Capa 2 (mac-filter), el cliente pasa a la seguridad de la Capa 3 (webauth-on-macfilter-failure).

## ¿Funciona correctamente el cliente si el explorador está configurado para el servidor proxy?

Antes de la versión 7.0, el cliente no podía establecer una conexión TCP cuando se configuraba el servidor proxy en el navegador. Después de la versión 7.0, se agrega esta compatibilidad con el servidor WebAuth Proxy y se pueden configurar la dirección IP y el puerto del servidor Proxy en el controlador.

## ¿Existe una guía de implementación para el acceso inalámbrico de invitados?

Este es el enlace a la guía de implementación:

Guía de implementación: Cisco Guest Access con el controlador de LAN inalámbrica de Cisco

## ¿Existe una guía de diseño para el acceso de invitados por cable e inalámbrico?

Estos son los enlaces a las guías de diseño:

- Servicios Cisco Unified Wireless Guest Access
- Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers

## Información Relacionada

- Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers
- Guía de implementación: Cisco Guest Access con el controlador de LAN inalámbrica de Cisco, versión 4.1
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).