Häufig gestellte Fragen zum Wireless-Gastzugriff

Inhalt

Einleitung

Dieses Dokument enthält Informationen zu den am häufigsten gestellten Fragen (FAQs) zum Wireless-Gastzugriff, der Teil des Cisco Unified Wireless-Netzwerks ist.

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Was ist ein Ethernet-over-IP (EoIP)-Tunnel zum ungesicherten Netzwerkbereich?

Cisco empfiehlt die Verwendung eines dedizierten Controllers für den Gastdatenverkehr. Dieser Controller wird als Guest Anker Controller bezeichnet.

Der Guest Anker Controller befindet sich in der Regel in einem ungesicherten Netzwerkbereich, der häufig als demilitarisierte Zone (DMZ) bezeichnet wird. Andere interne WLAN-Controller, von denen der Datenverkehr stammt, befinden sich im Unternehmens-LAN. Zwischen den internen WLAN-Controllern und dem Gast-Anker-Controller wird ein EoIP-Tunnel eingerichtet, um die Pfadisolierung des Gast-Datenverkehrs vom Enterprise-Datenverkehr sicherzustellen. Die Pfadisolierung ist eine wichtige Funktion zur Sicherheitsverwaltung für den Gastzugriff. Sie stellt sicher, dass Sicherheits- und Quality of Service (QoS)-Richtlinien getrennt sein können und zwischen Gast- und unternehmensinternem bzw. internem Datenverkehr unterschieden werden.

Ein wichtiges Merkmal der Cisco Unified Wireless Network-Architektur ist die Möglichkeit, mithilfe eines EoIP-Tunnels ein oder mehrere bereitgestellte WLANs (d. h. SSIDs) statisch einem bestimmten Gast-Anker-Controller im Netzwerk zuzuordnen. Der gesamte Datenverkehr - von und zu einem zugeordneten WLAN - durchläuft einen statischen EoIP-Tunnel, der zwischen einem Remote-Controller und dem Gast-Anker-Controller eingerichtet wird.

Auf diese Weise kann der gesamte Gastdatenverkehr transparent über das Unternehmensnetzwerk an einen Guest Anker Controller übertragen werden, der sich in einem ungesicherten Netzwerkbereich befindet.

Wie wähle ich den richtigen Controller für die Bereitstellung als Guest Anker Controller aus?

Die Auswahl des Gast-Anker-Controllers hängt von der Menge des Gast-Datenverkehrs ab, die durch die Anzahl der aktiven Gast-Client-Sitzungen bzw. durch die Uplink-Schnittstellenkapazität des Controllers definiert wird.

Der Gesamtdurchsatz und die Client-Einschränkungen pro Guest Anker Controller sind wie folgt:

- Cisco 2504 Wireless LAN Controller - 4 x 1-Gbit/s-Schnittstellen und 1.000 Gast-Clients
- Cisco 5508 Wireless LAN Controller (WLC) - 8 Gbit/s und 7.000 Gast-Clients
- Cisco Catalyst Wireless Services Module (WiSM-2) der Serie 6500 - 20 Gbit/s und 15.000 Clients
- Cisco 8500 Wireless LAN Controller (WLC) - 10 Gbit/s und 64.000 Clients

Hinweis: Die Cisco 7500 WLCs können nicht als Guest Anker Controller konfiguriert werden. Eine Liste der WLCs, die die Gastankerfunktion unterstützen, finden Sie unter Welche Controller können zur Unterstützung des Gastzugriffs im ungesicherten Netzwerkbereich verwendet werden?.

In der Datenbank jedes Controllers können maximal 2048 Gast-Benutzernamen und -Kennwörter gespeichert werden. Wenn die Gesamtzahl der aktiven Gastzugangsdaten diese Zahl übersteigt, ist daher mehr als ein Controller erforderlich. Gastanmeldeinformationen können auch auf einem externen RADIUS-Server gespeichert werden.

Die Anzahl der Access Points im Netzwerk hat keinen Einfluss auf die Auswahl des Guest Anker Controllers.

Wie viele Ethernet over IP (EoIP)-Tunnel können auf einem Guest Anker Controller terminiert werden?

Ein Gast-Anker-Controller kann bis zu 71 EoIP-Tunnel von internen WLAN-Controllern abschließen. Diese Kapazität ist für alle Cisco Wireless LAN Controller-Modelle bis auf den WLC-2504 identisch. Der Controller 2504 kann bis zu 15 EoIP-Tunnel terminieren. Wenn zusätzliche Tunnel erforderlich sind, können mehrere Guest Anker Controller konfiguriert werden.

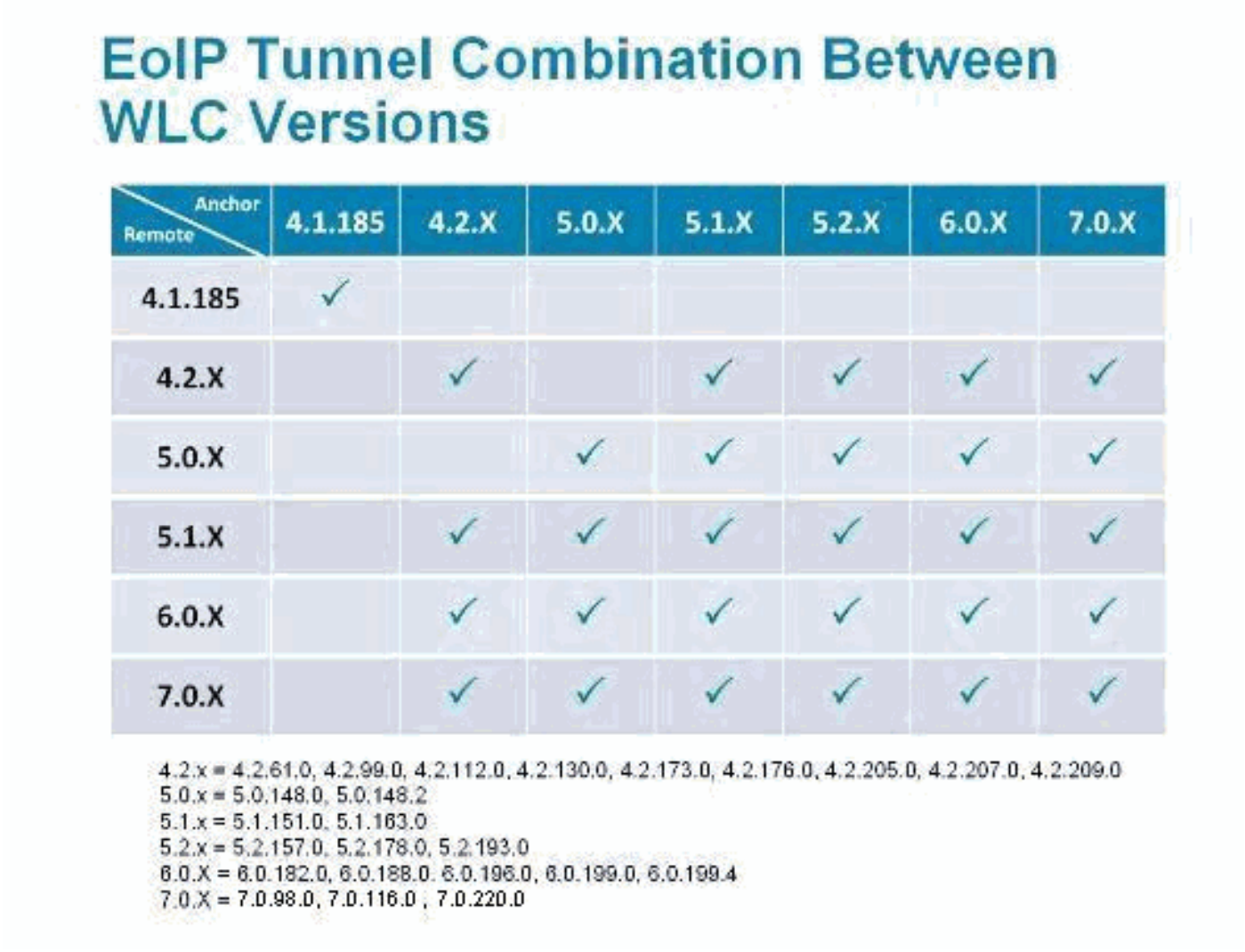
EoIP-Tunnel werden pro WLAN-Controller gezählt, unabhängig von der Anzahl an getunnelten WLANs oder Secure Set Identifiers (SSIDs) in jedem EoIP.

Zwischen dem Guest Anker Controller und jedem internen Controller wird ein EoIP-Tunnel konfiguriert, der Access Points mit Gast-Client-Zuordnungen unterstützt.

Kann ich Ethernet-over-IP (EoIP)-Tunnel zwischen Controllern mit unterschiedlichen Softwareversionen erstellen?

Dies wird nicht von allen Wireless LAN Controller-Softwareversionen unterstützt. In solchen Fällen sollte auf dem Remote- und Anker-Controller dieselbe Version der WLC-Software ausgeführt werden. Die aktuellen Softwareversionen erlauben es jedoch, dass die Remote- und Anker-Controller unterschiedliche Versionen haben.

In dieser Matrix sind die Softwareversionen der Wireless LAN Controller aufgeführt, mit denen Sie die EoIP-Tunnel erstellen können.



Kann der Cisco Wireless LAN Controller der Serien 2100/2500 als Gastgeber-Controller im ungesicherten Netzwerkbereich eingesetzt werden?

Ja, ab Version 7.4 der Cisco Unified Wireless Network Software kann der Cisco Wireless LAN Controller der Serie 2500 Gastdatenverkehr außerhalb der Firewall terminieren (bis zu 15 EoIP-Tunnel). Der Cisco Wireless LAN Controller der Serie 2000 kann nur Gast-Tunnel erstellen.

Kann das Cisco Wireless LAN Controller-Modul für Integrated Services Router (WLCM oder WLCM2) als Gastanker-Controller im ungesicherten Netzwerkbereich eingesetzt werden?

Nein, der WLCM oder WLCM2 kann Gasttunnel nicht terminieren. Der WLCM kann nur Gast-Tunnel erstellen.

Welche Controller können zur Unterstützung des Gastzugriffs in der ungesicherten Netzwerkzone verwendet werden?

Die Gast-Tunnel-Ankerfunktion, die EoIP-Tunnelterminierung, Webauthentifizierung und

Zugriffskontrolle für Gast-Clients umfasst, wird von den folgenden Cisco Wireless LAN Controller-Plattformen mit Software-Images der Version 4.0 oder höher unterstützt:

- Cisco Catalyst Wireless Services Module (WiSM2) der Serie 6500
- Cisco WiSM-2 Wireless LAN Controller
- Cisco Catalyst 3750G Integrierter Wireless LAN Controller
- Cisco Wireless LAN-Controller der 5508 Serie
- Cisco Wireless LAN Controller der Serie 2500 (Unterstützung ab Softwareversion 7.4)

Wenn ein Gast-Anker-Controller außerhalb der Firewall verwendet wird, welche Firewall-Ports sind für den Gastzugriff geöffnet?

Diese Ports müssen auf jeder Firewall zwischen dem Guest Anker Controller und den Remote-Controllern offen sein:

- Ältere Mobilität: IP-Protokoll 97 für Benutzerdatenverkehr, UDP-Port 16666
- Neue Mobilität: UDP-Port 16666 und 16667

Für eine optionale Verwaltung müssen diese Firewall-Ports offen sein:

- SSH/Telnet - TCP-Port 22/23
- TFTP - UDP-Port 69
- NTP - UDP-Port 123
- SNMP - UDP-Ports 161 (Gets und Sets) und 162 (Traps)
- HTTPS/HTTP - TCP-Port 443/80
- Syslog - TCP-Port 514
- RADIUS Auth/Account UDP-Port 1812 und 1813

Kann Gastdatenverkehr mit konfigurierter Network Address Translation (NAT) durch eine Firewall geleitet werden?

One-to-One NAT muss für den EoIP-Tunnel verwendet werden, der eine Firewall durchläuft.

Welcher WLC sendet im Szenario "Anchor - Foreign WLC" die RADIUS-Accounting-Informationen?

In diesem Szenario erfolgt die Authentifizierung immer über den Anker-WLC. Daher wird die RADIUS-Accounting vom Anker-WLC gesendet.

> **Hinweis**: In einer zentralen Bereitstellung für die Webauthentifizierung (CWA) und/oder Autorisierungsänderung (CoA) sollte die RADIUS-Kontoführung auf dem Anker DEAKTIVIERT und nur auf dem fremden WLC verwendet werden.

Der Gast-Tunnel zwischen internem Controller und Anker-

Controller funktioniert nicht. Diese Protokolle werden im WLC angezeigt: `mm_listen.c:5373 MM-3-INVALID_PKT_RECVD: Ein ungültiges Paket wurde vom 10.40.220.18 empfangen. Quellelement:0.0.0.0. Quellelement unbekannt.` Warum ist das so?

Sie überprüfen den Status des Tunnels über die WLC-GUI auf der Seite **WLANs**. Klicken Sie auf das Dropdown-Feld in der Nähe eines WLAN, und wählen Sie **Mobility Anchors** aus, das den Status der Steuerung und des Datenpfads enthält. Die Fehlermeldung wird aus einem der folgenden Gründe angezeigt:

1. Anker und interne Controller sind auf verschiedenen Versionen von Code. Stellen Sie sicher, dass die gleichen Codeversionen ausgeführt werden.
2. Fehlkonfigurationen in der Mobilitätsankerkonfiguration. Überprüfen Sie, ob die DMZ selbst als Mobilitätsanker konfiguriert ist und ob der DMZ-WLC in den internen WLCs als Mobilitätsanker konfiguriert ist. Weitere Informationen zur Konfiguration des Mobilitätsankers finden Sie im Abschnitt Configuring Auto- Anchor Mobility im Cisco Wireless LAN Controller Configuration Guide, Release 7.0. Dies führt dazu, dass Gastbenutzer den Datenverkehr nicht weiterleiten können.

Bei einer Einrichtung für den Wireless-Gastzugriff erhalten Clients die IP-Adresse nicht vom DHCP-Server. Die Fehlermeldung Do Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP dropping REPLY from Export-Foreign STA (DHCP aus Export-Ausland löschen) wird auf dem internen Controller angezeigt. Warum ist das so?

In einer Einrichtung für den Wireless-Gastzugriff müssen die DHCP-Proxyeinstellungen in den Guest Anchor-Controllern und dem internen Controller übereinstimmen. Andernfalls werden DHCP-Anfragen von Clients verworfen, und die folgende Fehlermeldung wird auf dem internen Controller angezeigt:

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

Verwenden Sie diesen Befehl, um die DHCP-Proxyeinstellung auf dem WLC zu ändern:

```
(Cisco Controller) >config dhcp proxy ?

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

Verwenden Sie den Befehl **show dhcp proxy** auf beiden Controllern, um sicherzustellen, dass beide Controller die gleiche DHCP-Proxy-Einstellung haben.

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

Wo erhalten Gastclients eine IP-Adresse, wenn Gastdatenverkehr über Tunnel in den ungesicherten Netzwerkbereich geleitet wird?

Gastdatenverkehr wird innerhalb des Unternehmens auf Layer 3 über EoIP transportiert. Daher können DHCP-Dienste (Dynamic Host Configuration Protocol) zunächst lokal auf dem Gast-Anker-Controller implementiert werden, oder der Gast-Anker-Controller kann Client-DHCP-Anfragen an einen externen Server weiterleiten. Dies ist auch die Methode, mit der die DNS-Adressauflösung (Domain Name System) behandelt wird.

Unterstützt der Cisco Wireless LAN Controller Webportale für die Gastauthentifizierung?

Die Cisco Wireless LAN Controller ab Version 3.2 bieten ein integriertes Webportal, in dem die Anmeldeinformationen von Gästen zur Authentifizierung erfasst werden. Es bietet einfache Branding-Funktionen sowie die Möglichkeit, Haftungsausschluss und Richtlinien zur akzeptablen Nutzung anzuzeigen.

Wie passe ich das Webportal an?

Informationen zum Anpassen eines Webportals finden Sie unter Auswählen der Webauthentifizierungs-Anmeldeseite.

Wie werden Gastanmeldeinformationen verwaltet?

Die Gastzugangsdaten können mit Cisco Wireless Control System (WCS) Version 7.0 und/oder Network Control System (NCS) Version 1.0 zentral erstellt und verwaltet werden. Netzwerkadministratoren können in WCS ein Administratorkonto mit eingeschränkten Rechten einrichten, das Lobbyisten-Zugriffsberechtigungen für die Erstellung von Gastanmeldeinformationen gewährt. In WCS oder NCS kann die Person mit einem Lobby-Ambassador-Konto Gastanmeldeinformationen für den Controller erstellen, zuweisen, überwachen und löschen, der als Guest Anker Controller fungiert.

Der Lobby-Botschafter kann den Gastbenutzernamen (oder die Benutzer-ID) und das Passwort eingeben, oder die Anmeldedaten werden automatisch generiert. Es gibt auch einen globalen Konfigurationsparameter, der die Verwendung eines Benutzernamens und eines Kennworts für alle Gäste oder eines eindeutigen Benutzernamens und Kennworts für jeden Gast ermöglicht.

Informationen zur Konfiguration des Lobby-Ambassador-Kontos auf dem WCS finden Sie im Abschnitt Creating Guest User Accounts (Erstellen von Gastbenutzerkonten) im Cisco Wireless Control System Configuration Guide, Release 7.0.

Ist die Lobby Ambassador-Funktion im Cisco Wireless LAN Controller zusätzlich zum Wireless Control System (WCS) oder NCS verfügbar?

Ja. Wenn WCS oder NCS nicht bereitgestellt wird, kann ein Netzwerkadministrator ein Lobby-Ambassador-Konto auf dem Guest Anker Controller einrichten. Eine Person, die sich über das Lobby-Ambassador-Konto beim Guest Anker Controller anmeldet, hat nur Zugriff auf die Funktionen zur Gastbenutzerverwaltung.

Wenn mehrere Guest Anker Controller vorhanden sind, muss ein WCS oder NCS verwendet werden, um Benutzernamen auf mehreren Guest Anker Controllern gleichzeitig zu konfigurieren.

Weitere Informationen zum Erstellen von Lobby Ambassador-Konten mit Wireless LAN Controllern finden Sie im Abschnitt Creating a Lobby Ambassador Account (Erstellen eines Lobby Ambassador-Kontos) im Cisco Wireless LAN Controller Configuration Guide, Release 7.0.

Können Gäste mit einem externen AAA-Server (Authentication, Authorization und Accounting) authentifiziert werden?

Ja. Anforderungen für die Gastauthentifizierung können an einen externen RADIUS-Server weitergeleitet werden.

Was passiert, wenn sich ein Gast anmeldet?

Wenn sich ein Wireless-Gast über das Webportal anmeldet, verarbeitet der Gast-Anker-Controller die Authentifizierung wie folgt:

1. Der Gast-Anker-Controller überprüft seine lokale Datenbank auf Benutzernamen und Kennwort und gewährt, falls vorhanden, Zugriff.
2. Wenn auf dem Gast-Anker-Controller lokal keine Benutzeranmeldeinformationen vorhanden sind, überprüft der Gast-Anker-Controller die WLAN-Konfigurationseinstellungen, um festzustellen, ob ein externer RADIUS-Server für das Gast-WLAN konfiguriert wurde. In diesem Fall erstellt der Controller ein RADIUS-Zugriffs-Anforderungspaket mit dem Benutzernamen und dem Kennwort und leitet es zur Authentifizierung an den ausgewählten RADIUS-Server weiter.
3. Wenn keine bestimmten RADIUS-Server für das WLAN konfiguriert wurden, überprüft der Controller die globalen Konfigurationseinstellungen des RADIUS-Servers. Alle externen RADIUS-Server, die mit der Option zur Authentifizierung des "Netzwerkbenutzers" konfiguriert , werden mit den Anmeldeinformationen des Gastbenutzers abgefragt. Andernfalls schlägt die Authentifizierung fehl, wenn auf keinem Server "Netzwerkbenutzer" ausgewählt ist und der Benutzer nicht über die Schritte 1 oder 2 authentifiziert wurde.

Ist es möglich, die Gastbenutzerauthentifizierung zu überspringen und nur die Option zum Haftungsausschluss für die Webseite anzuzeigen?

Ja. Eine weitere Konfigurationsoption für den Wireless-Gastzugriff besteht darin, die Benutzerauthentifizierung vollständig zu umgehen und den offenen Zugriff zu ermöglichen. Es kann jedoch erforderlich sein, vor der Gewährung des Zugriffs eine Seite mit einer Richtlinie zur akzeptablen Nutzung und einer Haftungsausschlussseite für Gäste bereitzustellen. Hierzu kann ein Gast-WLAN für den Web Policy Passthrough konfiguriert werden. In diesem Szenario wird ein

Gastbenutzer zu einer Webportalseite umgeleitet, die Haftungsausschlussinformationen enthält. Um die Identifizierung des Gastbenutzers zu ermöglichen, bietet der Passthrough-Modus dem Benutzer außerdem die Möglichkeit, vor dem Herstellen der Verbindung eine E-Mail-Adresse einzugeben.

Müssen der Remote-Controller und der Guest-Anker-Controller Teil derselben Mobilitätsgruppe sein?

Nein. Der Gast-Anker-Controller und der Remote-Controller können sich in separaten Mobilitätsgruppen befinden.

Wenn es mehr als eine Gast-SSID gibt, kann dann jedes WLAN (SSID) an ein eindeutiges Webseitenportal weitergeleitet werden?

Ja. Der gesamte Gastdatenverkehr in einem oder mehreren WLANs wird auf eine Webseite umgeleitet. Ab WLC Version 4.2 oder höher kann jedes WLAN auf eine eindeutige Webportalseite weitergeleitet werden. Weitere Informationen finden Sie im Abschnitt Assigning Login, Login Failure, and Logout Pages per WLAN im Cisco Wireless LAN Controller Configuration Guide, Release 7.0.

Welche Funktionen bietet die neue Einstellung in WLC Release 7.0, WebAuth on Mac Filter Failure?

Wenn für ein WLAN sowohl Layer-2- (MAC-Filter) als auch Layer-3-Sicherheit (Web-Authentifizierung-bei-Mac-Filter-Fehler) konfiguriert ist, wechselt der Client in den RUN-Status, wenn eine dieser beiden Optionen überschritten wird. Wenn die Layer-2-Sicherheit (MAC-Filter) ausfällt, wird der Client in die Layer-3-Sicherheit verschoben (Webauth-on-Macfilter-Failure).

Funktioniert der Client ordnungsgemäß, wenn der Browser für den Proxyserver konfiguriert ist?

Vor Version 7.0 konnte der Client keine TCP-Verbindung herstellen, wenn der Proxyserver im Browser konfiguriert wurde. Nach Version 7.0 wird diese WebAuth Proxy-Serverunterstützung hinzugefügt, und die IP-Adresse und der Port des Proxyservers können auf dem Controller konfiguriert werden.

Gibt es einen Bereitstellungsleitfaden für Wireless-Gastzugriff?

Dies ist der Link zum Bereitstellungsleitfaden:

Bereitstellungsleitfaden: Cisco Gastzugriff mit dem Cisco Wireless LAN Controller

Gibt es einen Designleitfaden für kabelgebundenen und

Wireless-Gastzugriff?

Dies sind die Links zu den Designleitfäden:

- Cisco Unified Wireless-Services für Gastzugriff
- Konfigurationsbeispiel für kabelgebundenen Gastzugriff mit Cisco WLAN-Controllern

Zugehörige Informationen

- **Konfigurationsbeispiel für kabelgebundenen Gastzugriff mit Cisco WLAN-Controllern**
- **Bereitstellungsleitfaden: Cisco Guest Access Using Cisco Wireless LAN Controller, Version 4.1**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.