

Konfigurationsbeispiel für kabelgebundenen Gastzugriff mit Cisco WLAN-Controllern

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Access Layer Switch-Konfiguration](#)

[Wichtige Punkte für die Bereitstellung von kabelgebundenen Gastgeräten](#)

[Plattformunterstützung](#)

[Wireless LAN-Konfiguration](#)

[Kabelgebundener Gastzugriff mit Anchor WLAN Controller](#)

[Konfiguration des kabelgebundenen Gastclients](#)

[Debugger für kabelgebundene Gastverbindungen auf lokalem WLC](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

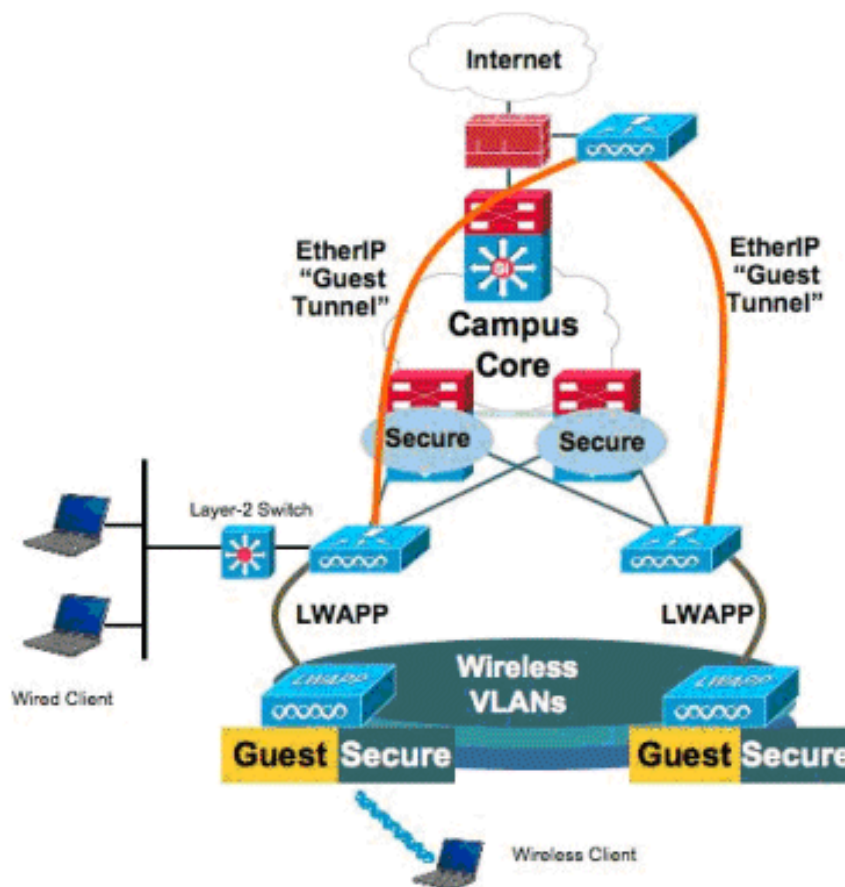
Einführung

In diesem Dokument wird beschrieben, wie Sie den Gastzugriff mithilfe der neuen Funktion für kabelgebundenen Gastzugriff auf den Cisco WLAN Controllern (WLCs) konfigurieren, die Cisco Unified Wireless Software Version 4.2.61.0 und höher verwenden. Immer mehr Unternehmen erkennen die Notwendigkeit an, ihren Kunden, Partnern und Beratern beim Besuch ihrer Einrichtungen Internetzugang bereitzustellen. IT-Manager können Gästen über denselben Wireless LAN-Controller sicheren und kontrollierten Zugriff auf das Internet über kabelgebundene und Wireless-Netzwerke bereitstellen.

Gastbenutzer müssen die Möglichkeit haben, eine Verbindung zu bestimmten Ethernet-Ports herzustellen und auf das Gastnetzwerk zuzugreifen, wie vom Administrator konfiguriert, nachdem sie die konfigurierten Authentifizierungsmethoden abgeschlossen haben. Wireless-Gastbenutzer können über die aktuellen Gastzugriffsfunktionen problemlos eine Verbindung zu den WLAN-Controllern herstellen. Darüber hinaus bietet das Wireless Control System (WCS) zusammen mit der grundlegenden Konfiguration und Verwaltung der WLAN-Controller erweiterte Gastbenutzerdienste. Kunden, die bereits WLAN-Controller und WCS in ihrem Netzwerk implementiert haben oder planen, können dieselbe Infrastruktur für den kabelgebundenen Gastzugriff nutzen. So wird Endbenutzern ein einheitlicher, kabelgebundener und Wireless-Gastzugriff ermöglicht.

Kabelgebundene Gastports werden an einem festgelegten Standort bereitgestellt und an einen Access Switch angeschlossen. Bei der Konfiguration auf dem Access Switch befinden sich diese Ports in einem der kabelgebundenen Layer-2-VLANs für Gäste. Den Kunden stehen zwei separate Lösungen zur Verfügung:

- Ein einzelner WLAN-Controller (VLAN Translation Mode) - Der Access Switch leitet den kabelgebundenen Gastdatenverkehr im Gast-VLAN an den WLAN-Controller weiter, der die kabelgebundene Gastzugangslösung bereitstellt. Dieser Controller übernimmt die VLAN-Übersetzung vom Eingangs-VLAN für kabelgebundene Gäste zum Ausgangs-VLAN.
- Zwei WLAN-Controller (Auto-Anchor-Modus): Der Access Switch leitet den kabelgebundenen Gastdatenverkehr an einen lokalen WLAN-Controller (den Controller, der dem Access Switch am nächsten liegt) weiter. Dieser lokale WLAN-Controller verankert den Client an einem DMZ-Anker-WLAN-Controller (Demilitarized Zone), der für den kabelgebundenen und Wireless-Gastzugriff konfiguriert ist. Nach erfolgreicher Übergabe des Clients an den DMZ-Anker-Controller werden die DHCP-IP-Adresszuweisung, die Client-Authentifizierung usw. im DMZ-WLC behandelt. Nach Abschluss der Authentifizierung kann der Client Datenverkehr senden/empfangen.



Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Unterstützung der Funktion für kabelgebundenen Gastzugriff auf den Cisco WLAN-Controllern wird von der Cisco Unified Wireless Software Version 4.2.61.0 und höher unterstützt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Access Layer Switch-Konfiguration

Um den kabelgebundenen Gastzugriff bereitzustellen, müssen die Ports im Access Layer-Switch für Layer 2 vom Administrator im Gast-VLAN konfiguriert werden. Das Gast-VLAN muss von allen anderen VLANs getrennt sein, die auf diesem Switch konfiguriert sind. Der Gast-VLAN-Datenverkehr wird an den nächsten lokalen WLAN-Controller weitergeleitet. Der lokale Controller leitet den Gastdatenverkehr über einen Ethernet over IP (EoIP)-Tunnel an einen DMZ Anchor-Controller weiter. Diese Lösung erfordert mindestens zwei Controller.

Alternativ dazu übersetzt der Access Switch das Gast-VLAN mit dem einzelnen Controller in die Ausgangsschnittstelle des WLAN-Controllers.

```
cat6506# show vlan id 49
```

VLAN	Name	Status	Ports
49	VLAN0049	active	Gi2/1, Gi2/2, Gi2/4, Gi2/35 Gi2/39, Fa4/24

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
49	enet	100049	1500	-	-	-	-	-	0	0

```
Remote SPAN VLAN
```

```
-----  
Disabled
```

Primary	Secondary	Type	Ports
---------	-----------	------	-------

```
cat6506#  
interface FastEthernet4/24  
  description Wired Guest Access  
  switchport  
  switchport access vlan 49  
  no ip address  
end  
cat6506#  
interface GigabitEthernet2/4  
  description Trunk port to the WLC  
  switchport  
  switchport trunk native vlan 80  
  switchport trunk allowed vlan 49,80,110  
  switchport mode trunk  
  no ip address  
end
```

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Wichtige Punkte für die Bereitstellung von kabelgebundenen Gastgeräten

- Derzeit werden fünf Gast-LANs für den kabelgebundenen Gastzugriff unterstützt. Insgesamt können im Anchor-WLC 16 WLANs für Wireless-Benutzer und 5 WLANs für kabelgebundenen Gastzugriff konfiguriert werden. Für WLANs gibt es keine separaten Tunnel. Alle Gast-WLANs, einschließlich der WLANs für kabelgebundenen Gastzugriff, verwenden dieselben EoIP-Tunnel zum Anchor-WLC.
- Administratoren müssen dynamische Schnittstellen im WLAN-Controller erstellen, sie als "Gast-LAN" markieren und sie mit WLANs verknüpfen, die als Gast-LANs erstellt wurden.
- Stellen Sie sicher, dass die WLAN-Konfigurationen einschließlich der Authentifizierung auf dem Anker- und Remote-Controller identisch sind, um den Client-Datenverkehr weiterzuleiten.
- WLCs sollten über kompatible Softwareversionen verfügen. Stellen Sie sicher, dass die gleiche Hauptversion ausgeführt wird.
- Die Webauthentifizierung ist der Standardsicherheitsmechanismus, der in einem kabelgebundenen Gast-LAN verfügbar ist. Folgende Optionen sind derzeit verfügbar: Offen, Webauthentifizierung und Webpassthrough.
- Falls der EoIP-Tunnel zwischen dem Remote- und Anker-WLC ausfällt, wird die Client-Datenbank vom Anchor-WLC entfernt. Der Kunde muss sich erneut zuordnen und authentifizieren.
- Es wird keine Layer-2-Sicherheit unterstützt.
- Multicast-/Broadcast-Datenverkehr in den LANs für kabelgebundene Gäste wird verworfen.
- Die DHCP-Proxy-Einstellungen müssen auf dem Anker- und dem Remote-Controller identisch sein.

Für den kabelgebundenen Gast wird im Controller ein Timeout für Inaktivität ausgeführt. Wenn innerhalb der konfigurierten Zeit keine Pakete vom Client empfangen werden, wird der Client vom Controller entfernt. Wenn ein Client beim nächsten Mal eine ARP-Anforderung (Address Resolution Protocol) sendet, wird ein neuer Clienteintrag erstellt und entsprechend der Sicherheitskonfiguration in den Web Auth/Run-Status verschoben.

Plattformunterstützung

Der kabelgebundene Gastzugriff wird auf folgenden Plattformen unterstützt:

- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, Virtual WLC

Wireless LAN-Konfiguration

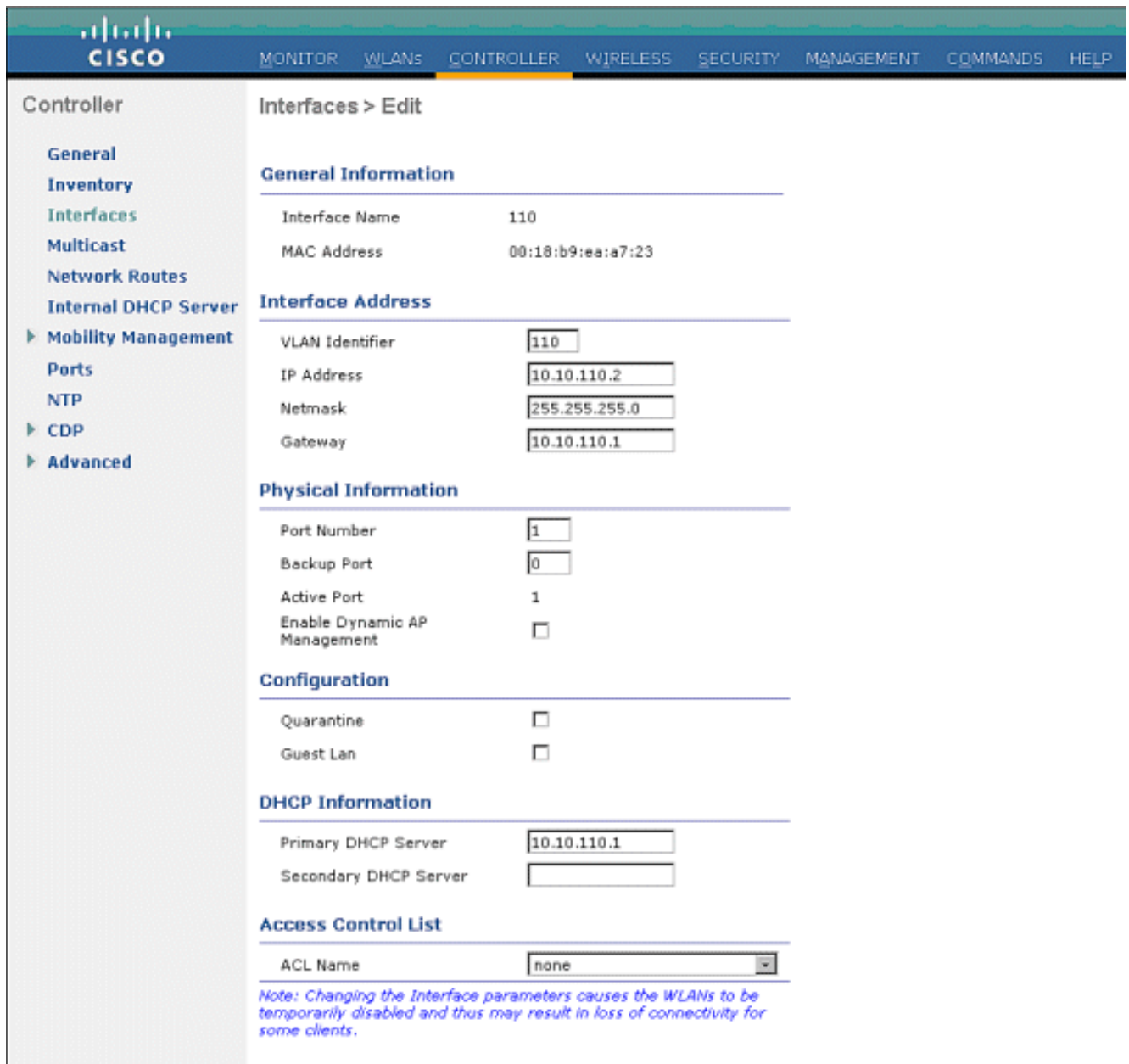
In diesem Beispiel wird von der grundlegenden Konfiguration des Wireless LAN-Controllers ausgegangen. Der Schwerpunkt liegt auf der zusätzlichen Konfiguration, die für die Implementierung des kabelgebundenen Gastzugriffs erforderlich ist.

1. Erstellen Sie eine dynamische Schnittstelle, und markieren Sie sie als "Gast-LAN". Wenn Sie diese dynamische Schnittstelle in der aktuellen Version erstellen, müssen Sie eine IP-Adresse und ein Standard-Gateway angeben, auch wenn diese Schnittstelle nicht vorhanden ist, da es sich um ein Layer-2-VLAN handelt. Sie müssen keine DHCP-Adresse angeben.

Kabelgebundene Gastclients sind physisch mit diesem VLAN verbunden.

The screenshot shows the Cisco Controller configuration interface for the 'wired-vlan-49' interface. The left sidebar contains a navigation menu with options like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > Edit' and is divided into several sections: 'General Information' (Interface Name: wired-vlan-49, MAC Address: 00:18:b9:ea:a7:23), 'Interface Address' (VLAN Identifier: 49, IP Address: 10.10.49.2, Netmask: 255.255.255.0, Gateway: 10.10.49.1), 'Physical Information' (Port Number: 1, Backup Port: 0, Active Port: 1, Enable Dynamic AP Management: unchecked), 'Configuration' (Quarantine: unchecked, Guest Lan: checked), 'DHCP Information' (Primary and Secondary DHCP Server fields), and 'Access Control List' (ACL Name: none). A note at the bottom states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

- Erstellen Sie eine weitere dynamische Schnittstelle, über die die kabelgebundenen Gastclients eine IP-Adresse erhalten. **Hinweis:** Sie müssen in dieser Schnittstelle eine IP-Adresse, ein Standard-Gateway und eine DHCP-Serveradresse angeben.



Controller

- General
- Inventory
- Interfaces
- Multicast
- Network Routes
- Internal DHCP Server
- ▶ Mobility Management
- Ports
- NTP
- ▶ CDP
- ▶ Advanced

Interfaces > Edit

General Information

Interface Name: 110
MAC Address: 00:18:b9:ea:a7:23

Interface Address

VLAN Identifier: 110
IP Address: 10.10.110.2
Netmask: 255.255.255.0
Gateway: 10.10.110.1

Physical Information

Port Number: 1
Backup Port: 0
Active Port: 1
Enable Dynamic AP Management:

Configuration

Quarantine:
Guest Lan:

DHCP Information

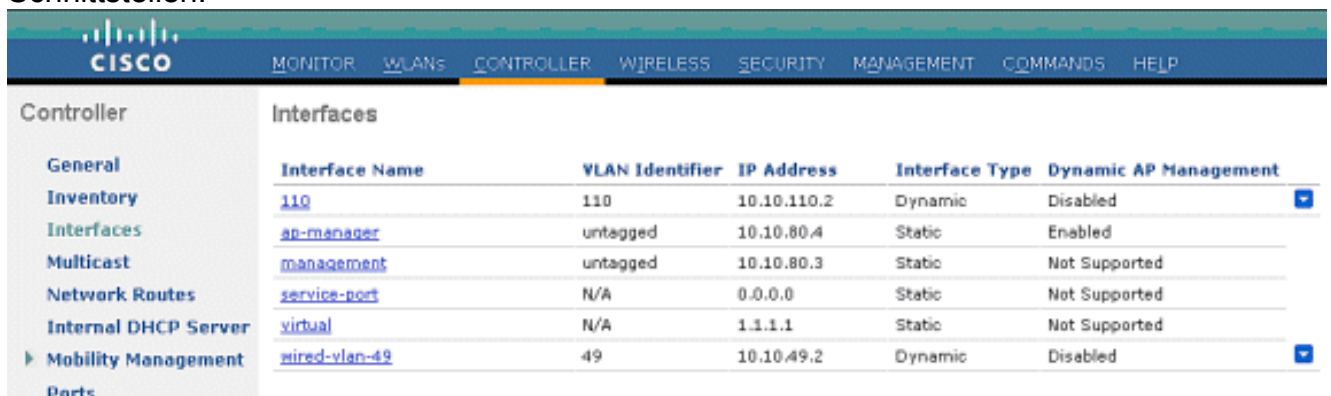
Primary DHCP Server: 10.10.110.1
Secondary DHCP Server:

Access Control List

ACL Name: none

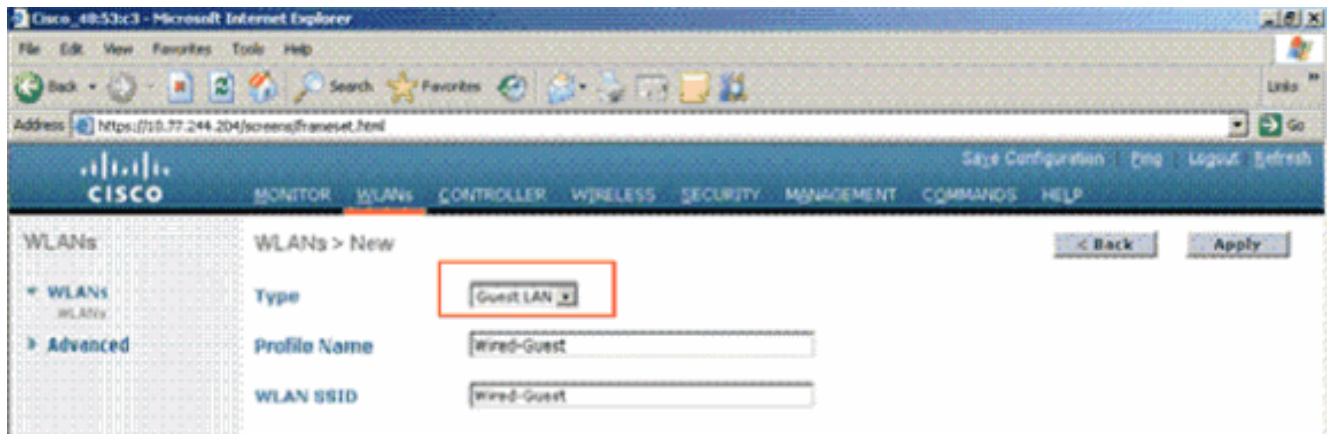
Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

3. Dies sind die dynamischen Schnittstellen:

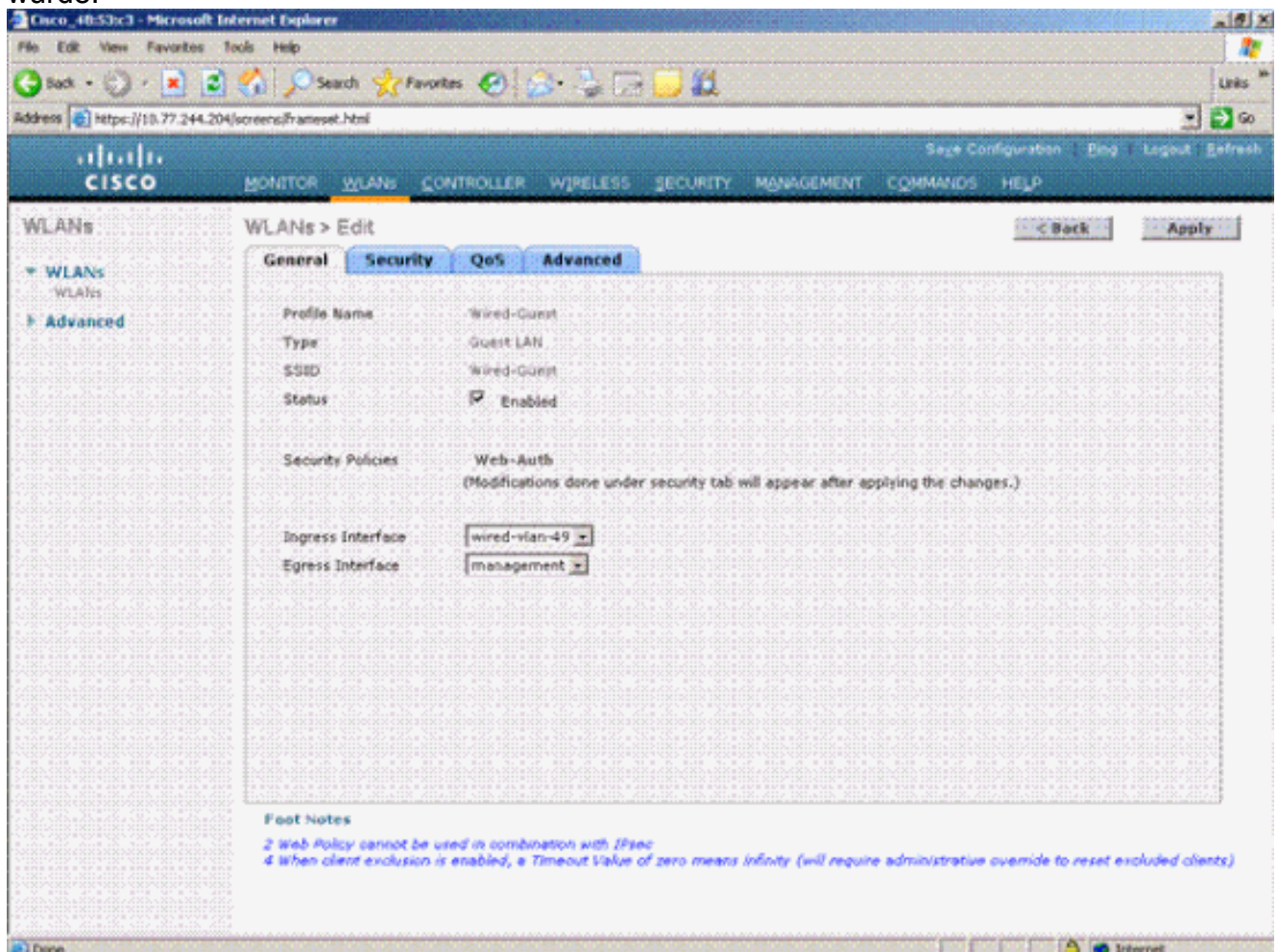


Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
110	110	10.10.110.2	Dynamic	Disabled
ap-manager	untagged	10.10.80.4	Static	Enabled
management	untagged	10.10.80.3	Static	Not Supported
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
wired-vlan-49	49	10.10.49.2	Dynamic	Disabled

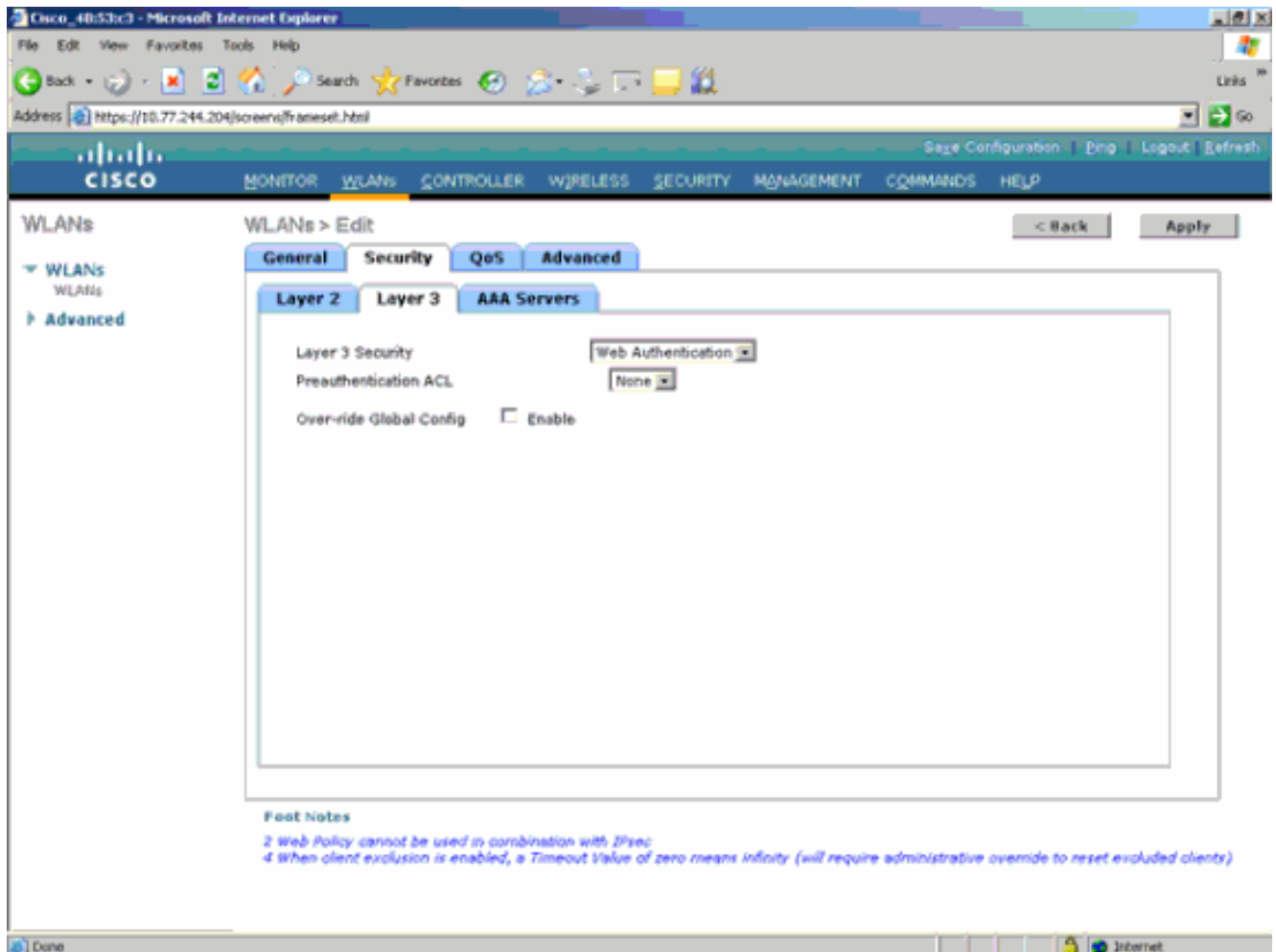
4. Hinzufügen eines neuen WLANs: Type=Gast-LAN



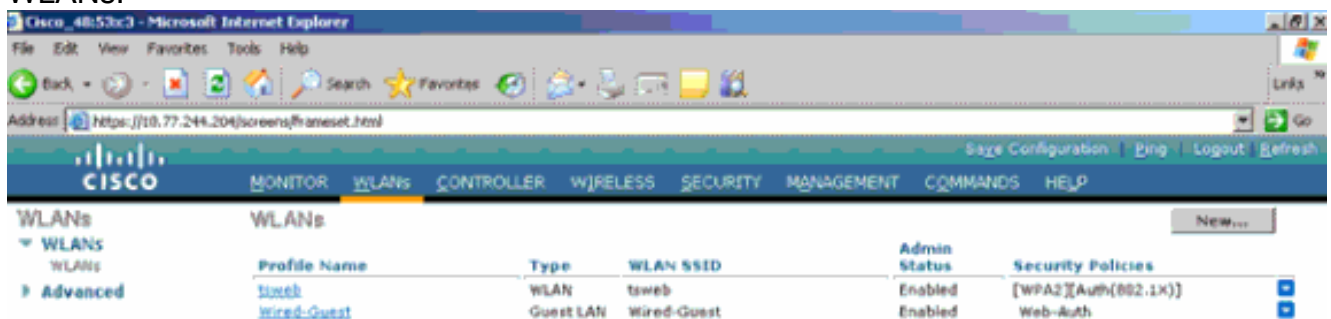
5. Aktivieren Sie das WLAN. Ordnen Sie die Eingangs-Schnittstelle dem in Schritt 1 erstellten "Gast-LAN" zu, und die Ausgangsschnittstelle kann eine Verwaltungsschnittstelle oder eine andere dynamische Schnittstelle sein, vorzugsweise aber eine dynamische Schnittstelle, wie sie in Schritt 2 erstellt wurde.



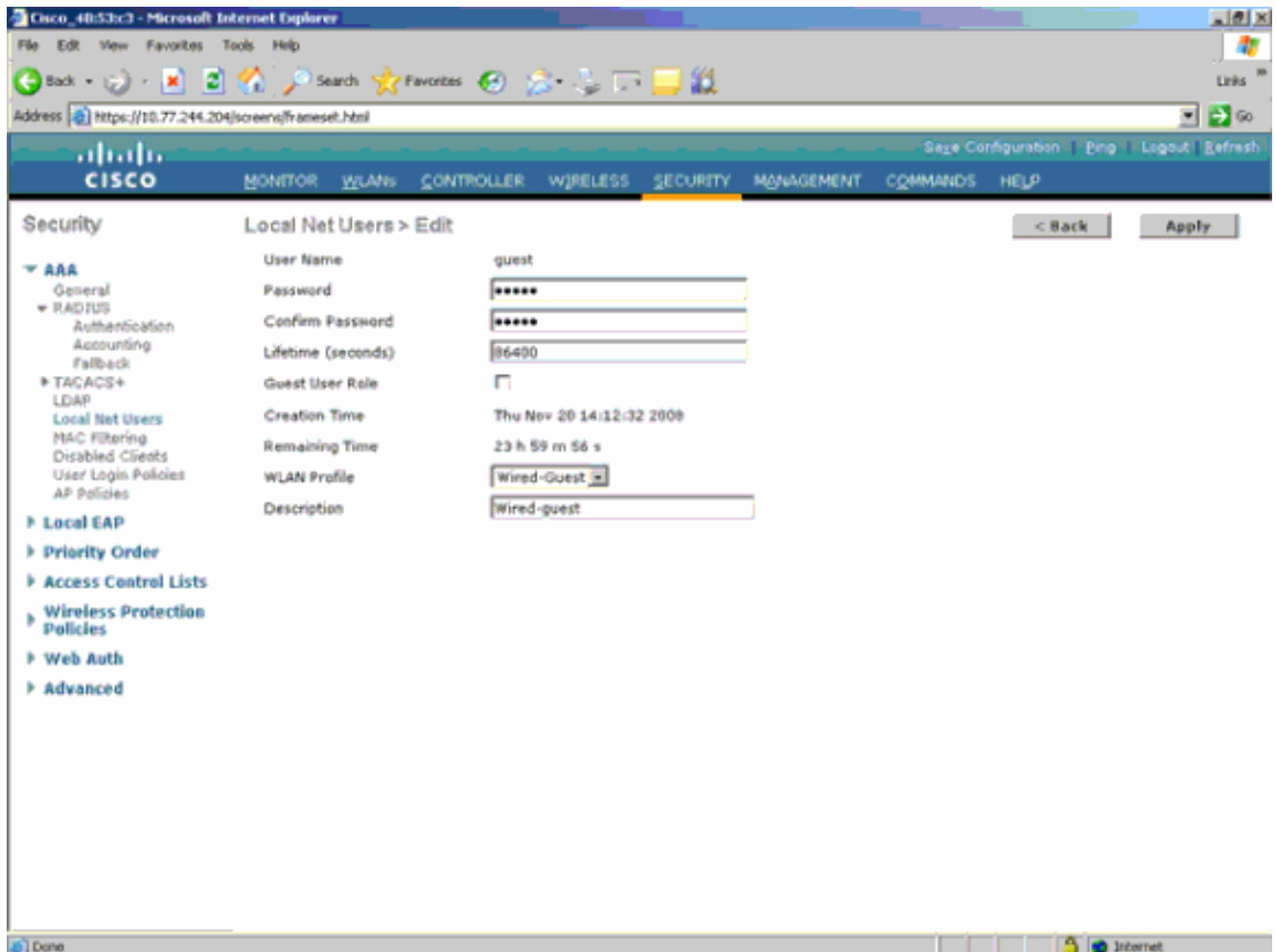
6. Die Webauthentifizierung ist standardmäßig als Sicherheitsoption im Gast-LAN aktiviert. Sie kann in *None* oder *Web Passthrough* geändert werden.



7. Dies ist die endgültige Konfiguration des WLANs.



8. Fügen Sie in der lokalen Datenbank des WLC einen Gastbenutzer hinzu.



Im Ausland müssen Sie den Eingang als konfiguriertes "Gast-LAN" festlegen. Am Ausgang müssen Sie eine Schnittstelle festlegen, möglicherweise die Management-Schnittstelle. Sobald der EoIP-Tunnel erstellt wurde, wird der Datenverkehr jedoch automatisch über den Tunnel anstatt über die Management-Adresse gesendet.

Kabelgebundener Gastzugriff mit Anchor WLAN Controller

In diesem Beispiel lautet die IP-Adresse des Remote-Wireless LAN-Controllers 10.10.80.3 und die IP-Adresse des Anchor DMZ-Controllers 10.10.75.2. Beide sind Teil zweier unterschiedlicher Mobilitätsgruppen.

1. Konfigurieren Sie die Mobilitätsgruppe des Anker DMZ-Controllers, wenn Sie die MAC-Adresse, die IP-Adresse und den Namen der Mobilitätsgruppe des Remote-Controllers hinzufügen.

The screenshot shows the Cisco Controller GUI with the 'CONTROLLER' tab selected. The left sidebar shows the navigation menu with 'Mobility Management' expanded to 'Mobility Groups'. The main content area is titled 'Mobility Group Members > Edit All'. Below the title is a text box explaining that the page allows editing all mobility group members at once, and each member is represented as a MAC address, IP address, and optional group name. A text area contains the following entries:

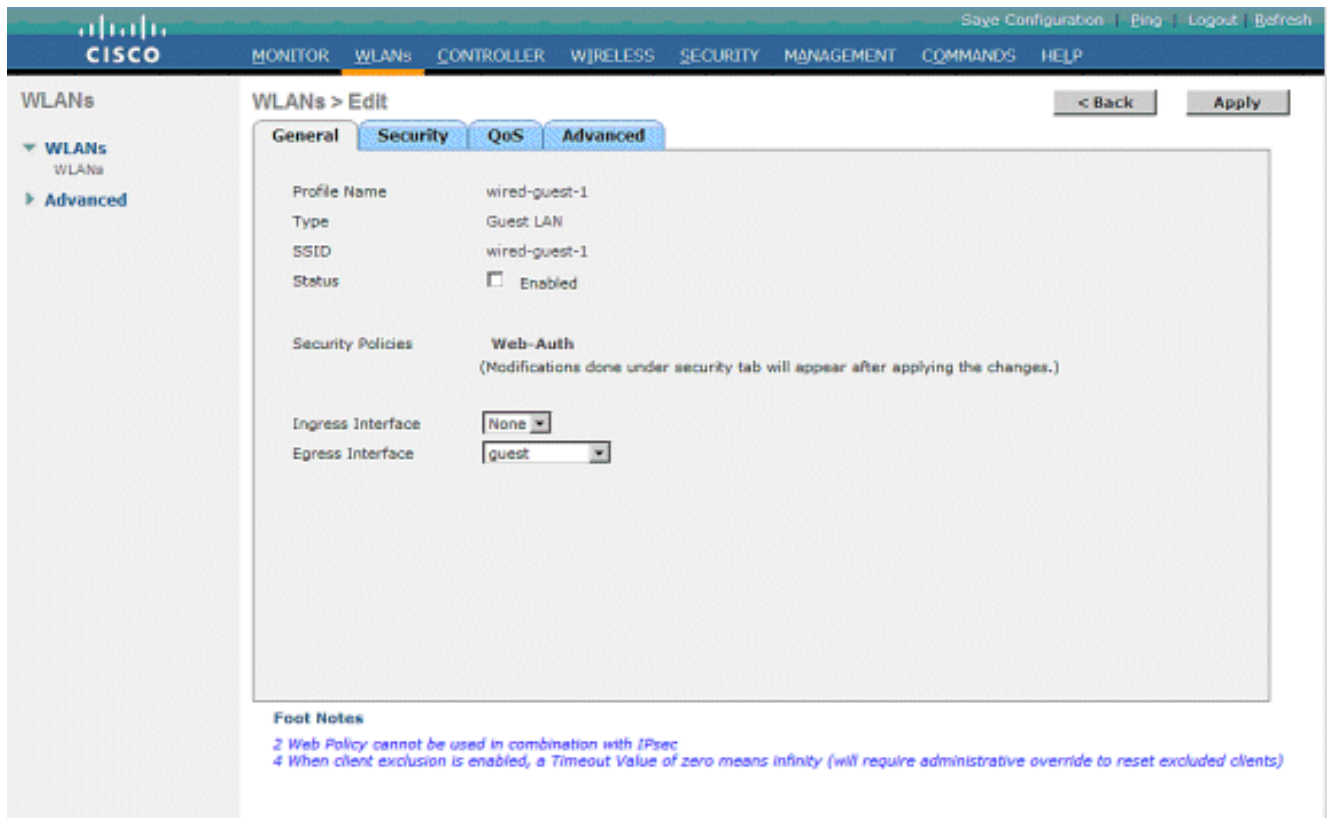
```
00:18:73:34:b2:60 10.10.75.2
00:18:b9:ea:a7:20 10.10.80.3 mobile-10
```

2. Konfigurieren Sie auf ähnliche Weise die Mobilitätsgruppe im Remote-Controller.

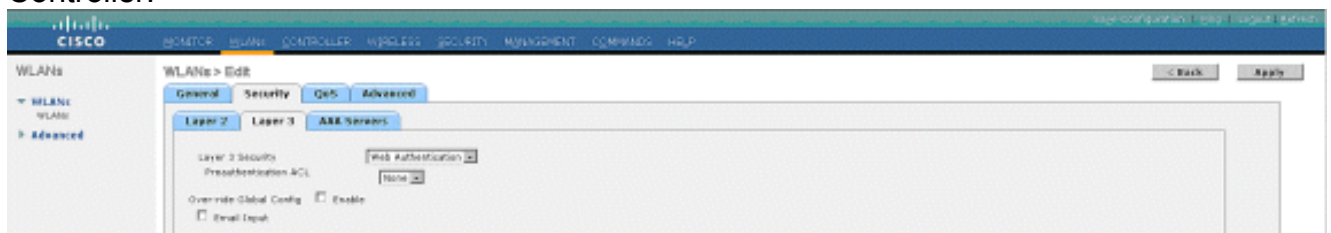
The screenshot shows the Cisco Controller GUI with the 'CONTROLLER' tab selected. The left sidebar shows the navigation menu with 'Mobility Management' expanded to 'Mobility Groups'. The main content area is titled 'Mobility Group Members > Edit All'. Below the title is a text box explaining that the page allows editing all mobility group members at once, and each member is represented as a MAC address, IP address, and optional group name. A text area contains the following entries:

```
00:18:b9:ea:a7:20 10.10.80.3
00:18:73:34:b2:60 10.10.75.2 mobile-9
```

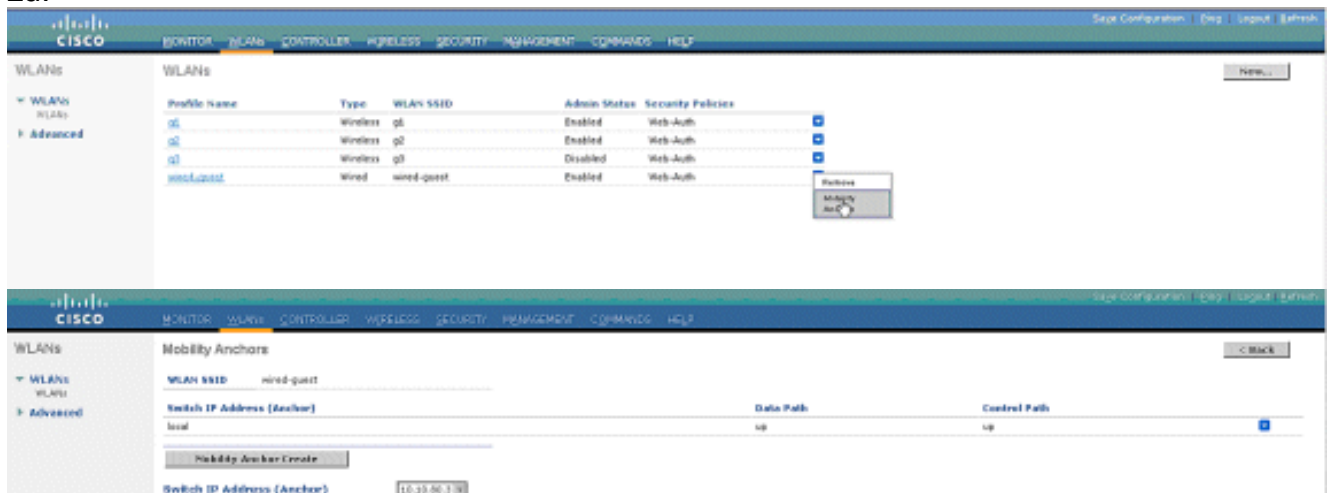
3. Erstellen Sie das kabelgebundene WLAN mit dem genauen Namen im Anchor-WLC. Die Eingangs-Schnittstelle ist in diesem Fall "none", da logischerweise die Eingangs-Schnittstelle der EoIP-Tunnel vom Remote-Controller ist. Die Ausgangsschnittstelle ist eine andere Schnittstelle, über die die kabelgebundenen Clients die IP-Adresse empfangen. In diesem Beispiel wird eine dynamische Schnittstelle mit dem Namen *guest* erstellt. In diesem Stadium können Sie das WLAN jedoch nicht aktivieren, da eine Fehlermeldung angezeigt wird, die besagt, dass eine Eingangsschnittstelle nicht *unbeschränkt* sein kann.



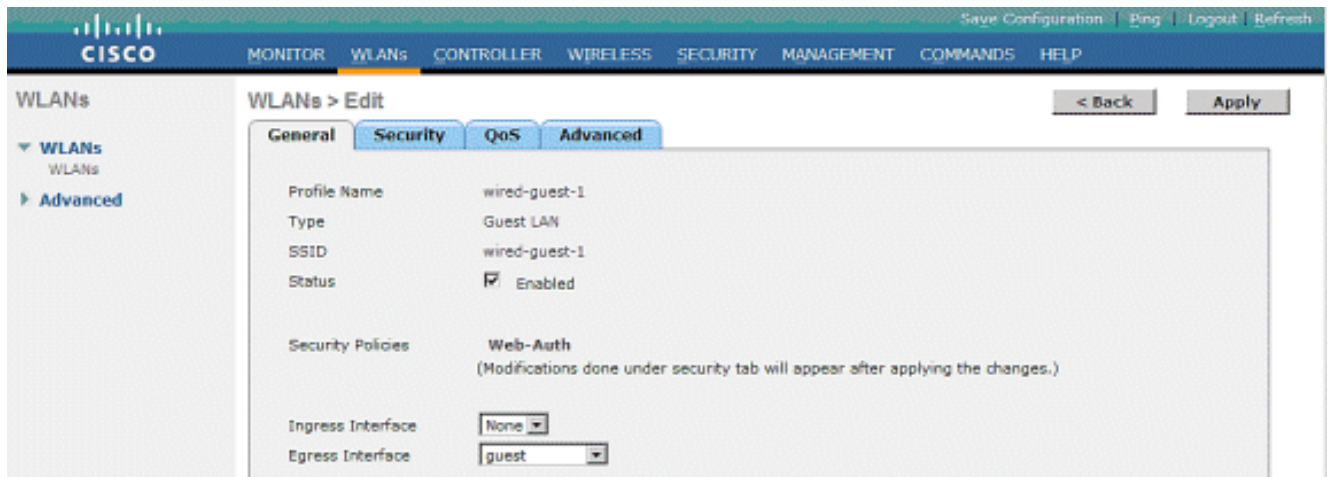
4. Konfigurieren Sie die Layer-3-Sicherheit als *Webauthentifizierung*, ähnlich dem Remote-Controller.



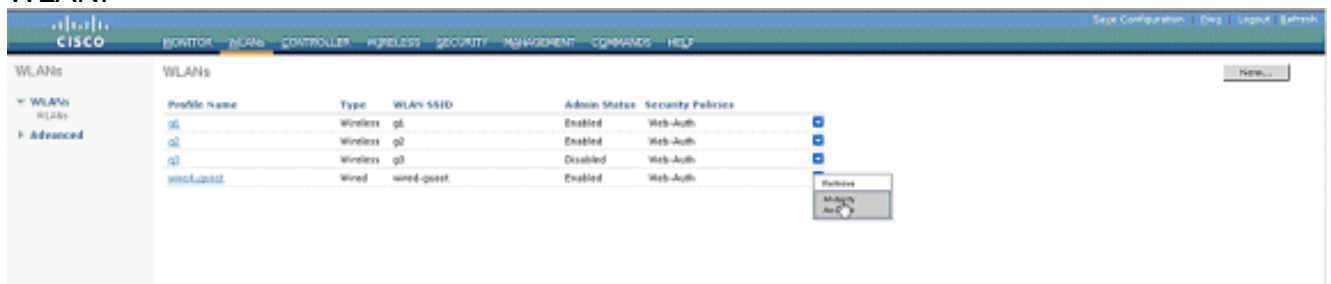
5. Erstellen Sie den Mobilitätsanker am Anker-Controller, und ordnen Sie ihn sich selbst zu.



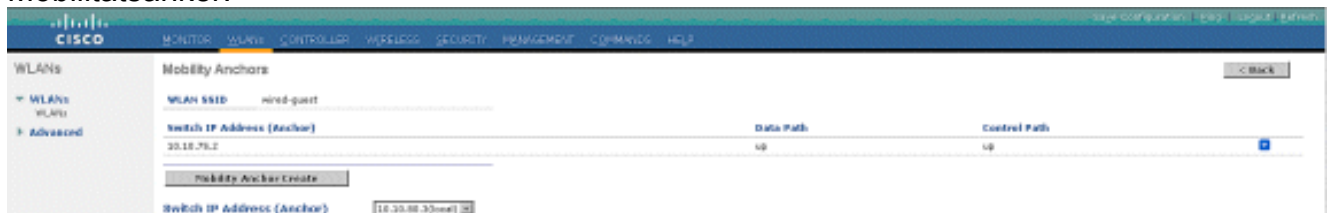
6. Wenn der Mobilitätsanker erstellt wurde, kehren Sie zurück, und aktivieren Sie das kabelgebundene WLAN.



7. Erstellen Sie auf ähnliche Weise den Mobilitätsanker auf dem Remote-WLC für das kabelgebundene Gast-WLAN.



Wählen Sie die IP-Adresse des Anker-WLC aus, und erstellen Sie den Mobilitätsanker.



Überprüfen Sie, ob der Daten- und Steuerungspfad aktiv ist. Falls nicht, stellen Sie sicher, dass diese Ports zwischen dem Anker und dem Remote-Wireless LAN-Controller offen sind: UDP 1666 oder IP 97.

8. Wenn ein kabelgebundener Gastbenutzer mit dem Switch verbunden ist und die Webauthentifizierung abgeschlossen hat, muss der Status "Policy Manager" ausgeführt werden, und die Rolle "Mobility" lautet "Export Foreign" (Ausländisch exportieren).

The screenshot shows the Cisco WLC Monitor interface. The left sidebar has a menu with 'Clients' selected. The main content area is titled 'Clients > Detail' and contains two tables: 'Client Properties' and 'AP Properties'. The 'Client Properties' table shows a regular client with MAC address 00:0d:60:5e:ca:62, IP address 0.0.0.0, and Policy Manager State 'RUN'. The 'AP Properties' table shows the client is associated with AP Name 'N/A' and WLAN Profile 'wired-guest-1'.

Client Properties		AP Properties	
MAC Address	00:0d:60:5e:ca:62	AP Address	Unknown
IP Address	0.0.0.0	AP Name	N/A
Client Type	Regular	AP Type	Unknown
User Name		WLAN Profile	wired-guest-1
Port Number	1	Status	Associated
Interface	110	Association ID	0
VLAN ID	110	802.11 Authentication	Open System
CCX Version	Not Supported	Reason Code	0
E2E Version	Not Supported	Status Code	0
Mobility Role	Export Foreign	CF Pollable	Not Implemented
Mobility Peer IP Address	10.10.75.2	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Not Implemented
Mirror Mode	Disable	PBCC	Not Implemented
Management Frame Protection	No	Channel Agility	Not Implemented
		Timeout	0

Überprüfen Sie auf ähnliche Weise den Status im Anchor-WLC. Der Status "Policy Manager" muss "RUN" lauten, und die Mobilitätsrolle "Export Anchor".

The screenshot shows the Cisco WLC Monitor interface for an anchor WLC. The left sidebar has a menu with 'Clients' selected. The main content area is titled 'Clients > Detail' and contains two tables: 'Client Properties' and 'AP Properties'. The 'Client Properties' table shows a mobile client with MAC address 00:0d:60:5e:ca:62, IP address 10.10.77.11, and Policy Manager State 'RUN'. The 'AP Properties' table shows the client is associated with AP Name '10.10.80.3' and WLAN Profile 'wired-guest-1'.

Client Properties		AP Properties	
MAC Address	00:0d:60:5e:ca:62	AP Address	Unknown
IP Address	10.10.77.11	AP Name	10.10.80.3
Client Type	Regular	AP Type	Mobile
User Name	guest	WLAN Profile	wired-guest-1
Port Number	1	Status	Associated
Interface	guest	Association ID	0
VLAN ID	77	802.11 Authentication	Open System
CCX Version	Not Supported	Reason Code	0
E2E Version	Not Supported	Status Code	0
Mobility Role	Export Anchor	CF Pollable	Not Implemented
Mobility Peer IP Address	10.10.80.3	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Not Implemented
Mirror Mode	Disable	PBCC	Not Implemented
Management Frame Protection	No	Channel Agility	Not Implemented
		Timeout	0

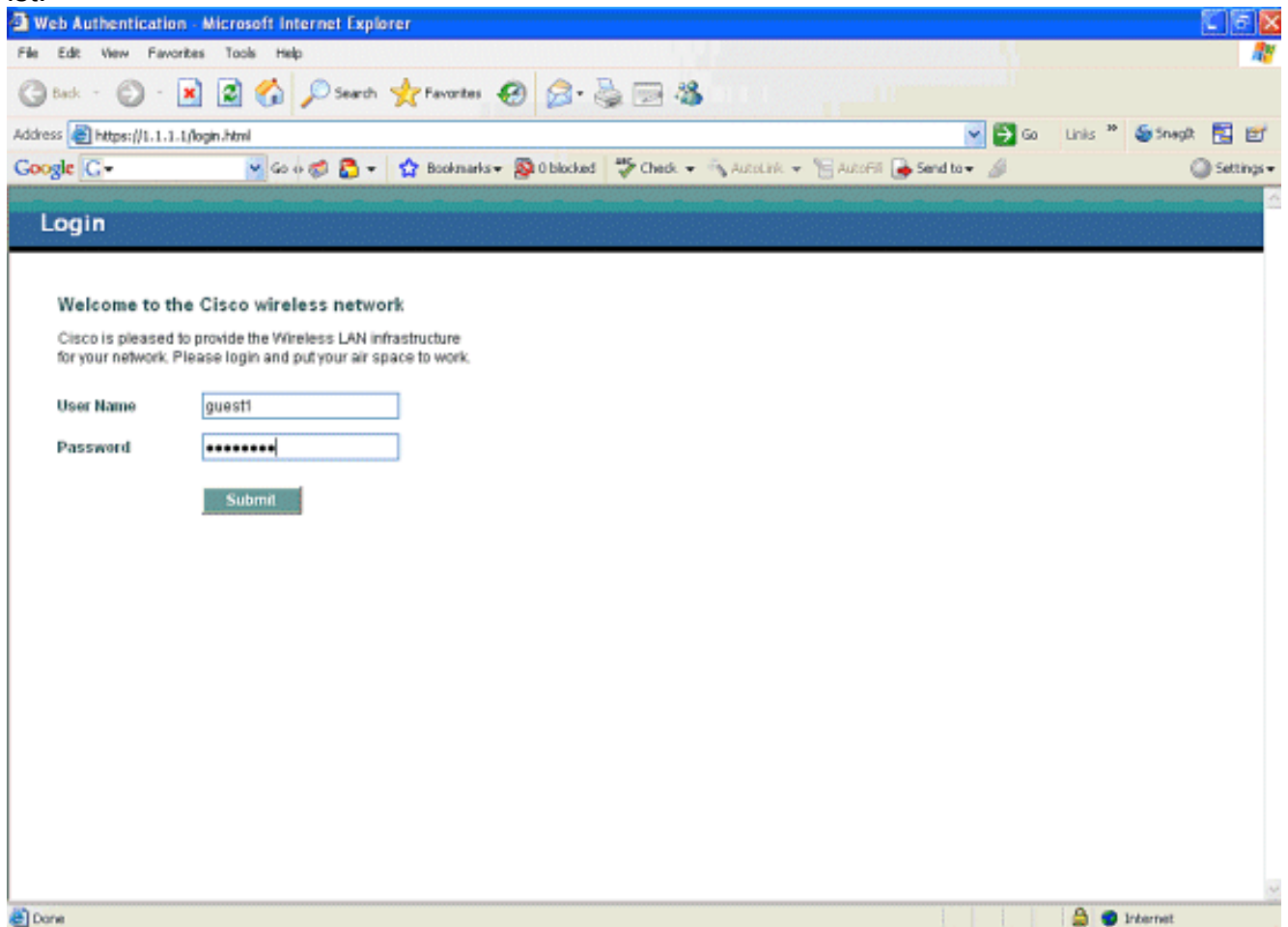
Konfiguration des kabelgebundenen Gastclients

Der kabelgebundene Gast-Client erhält eine IP-Adresse vom Ausgangs-VLAN, kann jedoch keinen Datenverkehr weiterleiten, bis der Webauthentifizierungsprozess abgeschlossen ist.

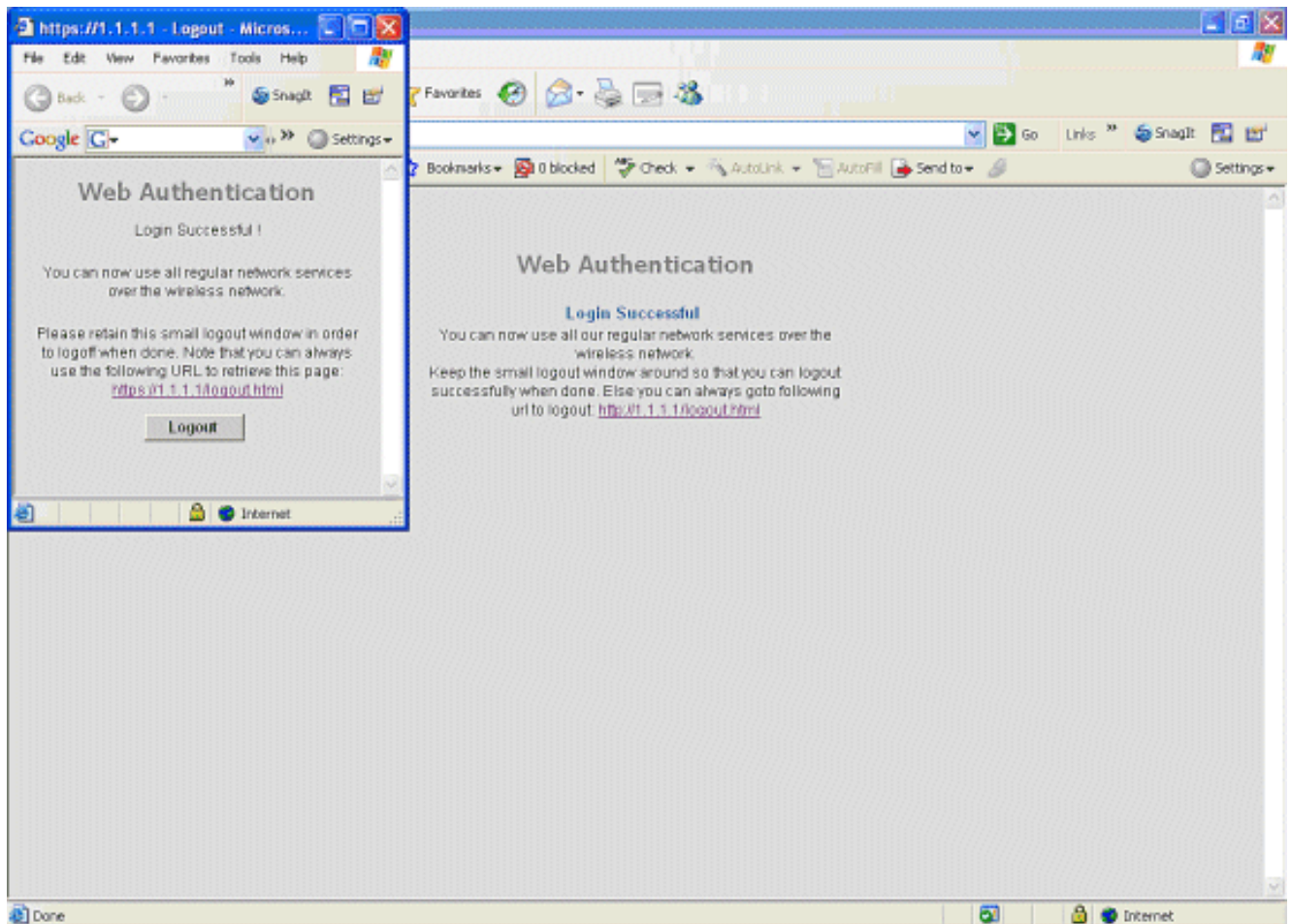
Um sich als Gastbenutzer anzumelden, gehen Sie wie folgt vor:

1. Öffnen Sie ein Browserfenster, und geben Sie den gewünschten URL-Namen ein (z. B. www.cisco.com). Wenn die Webauthentifizierung aktiviert ist, wird der Gast auf die Standardwebseite des Wireless LAN-Controllers umgeleitet, und für die eingegebene URL kann eine DNS-Auflösung vorgenommen werden. Geben Sie andernfalls die folgende URL ein: <https://1.1.1.1/login.html>, wobei die IP-Adresse 1.1.1.1 die virtuelle IP-Adresse des Wireless LAN-Controllers

ist.



2. Geben Sie den angegebenen Benutzernamen und das angegebene Kennwort ein.
3. Wenn die Anmeldung erfolgreich war, wird dies in einem Browserfenster angezeigt.



Debugger für kabelgebundene Gastverbindungen auf lokalem WLC

Dieses Debuggen stellt alle Informationen zum kabelgebundenen Gastclient bereit.

debug client

```

Cisco Controller) >show debug
MAC address ..... 00:0d:60:5e:ca:62
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.

(Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  Adding mobile on Wired Guest 00:00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
  apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
    00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated

```

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
 Initializing policy

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
 Change state to AUTHCHECK (2) last state AUTHCHECK (2)

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)
 Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)
 Change state to DHCP_REQD (7) last state DHCP_REQD (7)

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
 apfPemAddUser2 (apf_policy.c:209) Changing state for mobile
 00:0d:60:5e:ca:62 on AP 00:00:00:00:00:00 from Associated to Associated

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -
 not starting session timer for the mobile

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
 Stopping deletion of Mobile Station: (callerId: 48)

Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
 Wired Guest packet from 10.10.80.252 on mobile

Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
 Wired Guest packet from 10.10.80.252 on mobile

Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
 Orphan Packet from 10.10.80.252

Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
 Wired Guest packet from 169.254.20.157 on mobile

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
 Wired Guest packet from 169.254.20.157 on mobile

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
 **DHCP_REQD (7) State Update from Mobility-Incomplete
 to Mobility-Complete, mobility role=Local**

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
 DHCP_REQD (7) pemAdvanceState2 3934, Adding TMP rule

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
 DHCP_REQD (7) Adding Fast Path rule

type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,
 slot 0, interface = 1, QOS = 0 ACL Id = 255,
 Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP_REQD
 (7) Successfully plumbed mobile rule (ACL ID 255)

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
 Installing Orphan Pkt IP address 169.254.20.157 for station

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
 Unsuccessfully installed IP address 169.254.20.157 for station

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
 0.0.0.0 Added NPU entry of type 9

Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
 Sent an XID frame

Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62
 Wired Guest packet from 169.254.20.157 on mobile

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP selecting relay 1 - control block settings:
 dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
 dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 **DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
 gateway 10.10.110.1, VLAN 110, port 1)**

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP transmitting DHCP DISCOVER (1)

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP xid: 0x87214d01 (2267106561),secs: 0, flags: 8000

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
 DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP requested ip:10.10.80.252

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2
VLAN: 110

Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
DHCP selected relay 2 - NONE

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
gateway 10.10.110.1, VLAN 110, port 1)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP transmitting DHCP DISCOVER (1)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP requested ip: 10.10.80.252

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
DHCP selected relay 2 - NONE

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP setting server from OFFER
(server 10.10.110.1, yiaddr 10.10.110.3)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP sending REPLY to Wired Client (len 350, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP transmitting DHCP OFFER (2)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP xid: 0x87214d01 (2267106561), secs: 0, flags: 8000

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP ciaddr: 0.0.0.0, yiaddr: 10.10.110.3

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP server id: 1.1.1.1 rcvd server id: 10.10.110.1

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP selecting relay 1 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
gateway 10.10.110.1, VLAN 110, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP transmitting DHCP REQUEST (3)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP siaddr: 0.0.0.0, giaddr: 10.10.110.2

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP requested ip: 10.10.110.3

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP server id: 10.10.110.1 rcvd server id: 1.1.1.1

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP selecting relay 2 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP selected relay 2 -NONE

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 DHCP_REQD (7) Change state to WEBAUTH_REQD
(8) last state WEBAUTH_REQD (8)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_REQD (8) pemAdvanceState2
4598, Adding TMP rule

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_REQD (8) Replacing Fast Path rule
type = Airespace AP Client - ACL passthru
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_REQD (8) Successfully
plumbed mobile rule (ACL ID 255)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
Plumbing web-auth redirect rule due to user logout

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
Assigning Address 10.10.110.3 to mobile

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP sending REPLY to Wired Client (len 350, port 1)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP transmitting DHCP ACK (5)

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62


```

DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP ciaddr: 0.0.0.0, yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
DHCP server id: 1.1.1.1 rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Setting guest session timeout for mobile
00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
Session Timeout is 79953 - starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_REQD (8) Change state to
WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
10.10.110.3 WEBAUTH_NOL3SEC (14) Change state to RUN
(20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Replacing FastPath rule
type = Airespace AP Client
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
ARP for 10.10.110.3, VLAN Id 110

```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Konfigurieren von automatischer Ankermobilität](#)
- [Gast-WLAN und internes WLAN mit WLCs - Konfigurationsbeispiel](#)
- [Konfigurationsbeispiel für die externe Webauthentifizierung mit Wireless LAN-Controllern](#)

- [Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.2](#)
- [Wireless-Produktunterstützung](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)