采用融合接入的统一接入无线局域网控制器访客锚点配置示例

目录

简介

本文档介绍如何在新的移动部署设置中为无线客户端访客锚点配置5508/5760系列无线LAN控制器(WLC)和Catalyst 3850系列交换机，其中5508系列WLC充当移动锚点，而Catalyst 3850系列交换机充当客户端的移动外部控制器。此外，Catalyst 3850系列交换机作为移动代理连接到5760系列WLC，后者作为移动控制器，Catalyst 3850系列交换机从中获取接入点(AP)许可证。

先决条件

要求

Cisco 建议您在尝试进行此配置之前了解下列主题：

- 融合接入5760和3650系列WLC和Catalyst 3850系列交换机的Cisco IOS® GUI或CLI
- 5508系列WLC的GUI和CLI访问
- 服务集标识符(SSID)配置
- Web 身份验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 5760版本3.3.3（下一代配线间[NGWC]）
- Catalyst 3850 系列交换机
- 思科5508系列WLC版本7.6.120
- 思科3602系列轻量AP
- Cisco Catalyst 3560 系列交换机

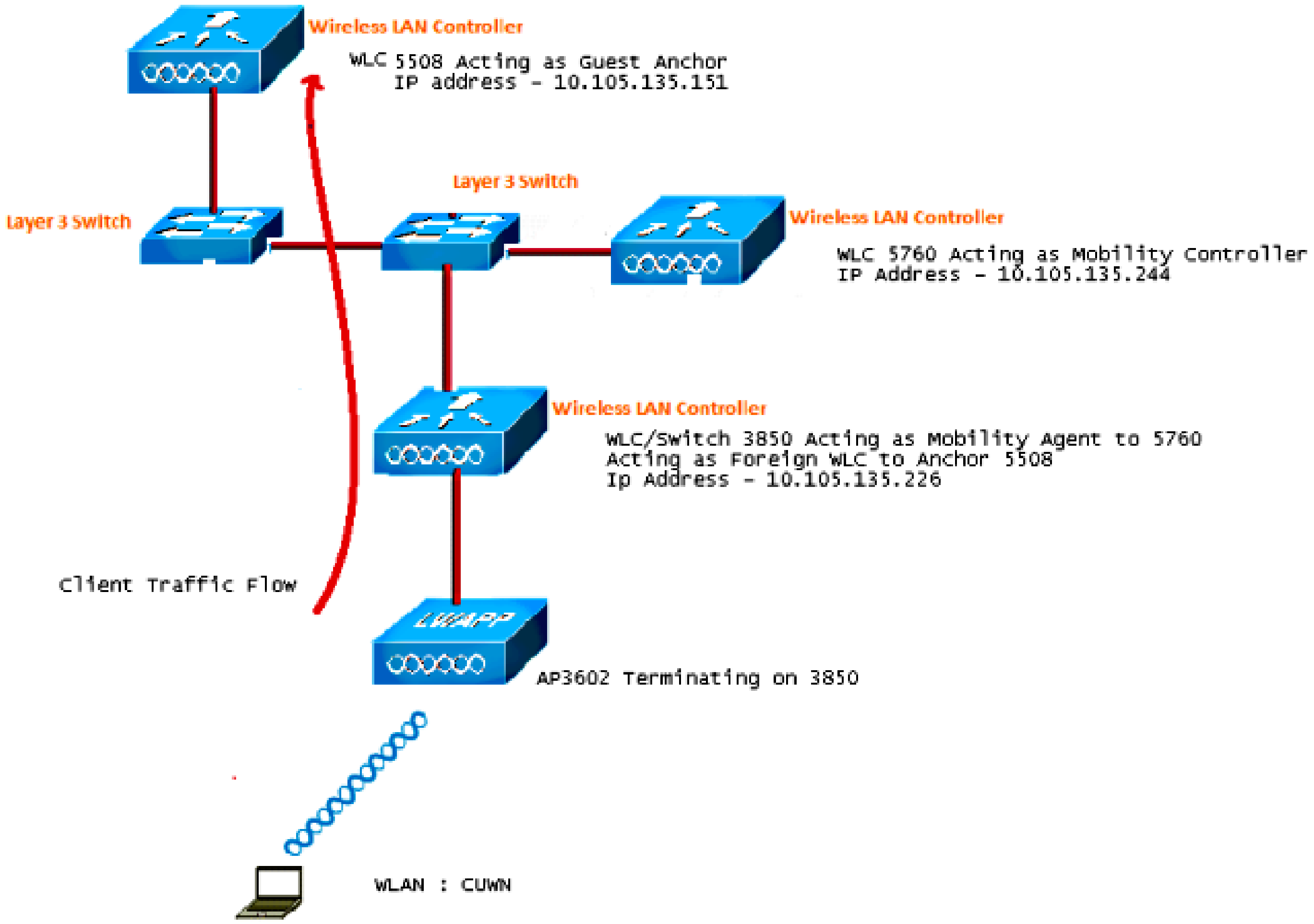
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

> **注意：要获取有关本部分中所使用命令的更多信息，可使用**命令查找工具（仅限已注册客户）。

网络图

5508系列WLC充当锚点控制器，Catalyst 3850系列交换机充当外部控制器和从移动控制器5760获取许可证的移动代理。


Wireless LAN Controller
WLC 5508 Acting as Guest Anchor
IP address - 10.105.135.151
Layer 3 Switch
Layer 3 Switch
Wireless LAN Controller
WLC 5760 Acting as Mobility Controller
IP Address - 10.105.135.244
Wireless LAN Controller
WLC/Switch 3850 Acting as Mobility Agent to 5760
Acting as Foreign WLC to Anchor 5508
Ip Address - 10.105.135.226
Client Traffic Flow
LWAPP
AP3602 Terminating on 3850
WLAN : CUWN

注：在网络图中，5508系列WLC充当锚点控制器，5760系列WLC充当移动控制器，Catalyst 3850系列交换机充当移动代理和外部WLC。在任何时间点，Catalyst 3850系列交换机的锚点控制器是5760系列WLC或5508系列WLC。两个锚点不能同时为锚点，因为双锚点不起作用。

配置

配置包括三个部分：

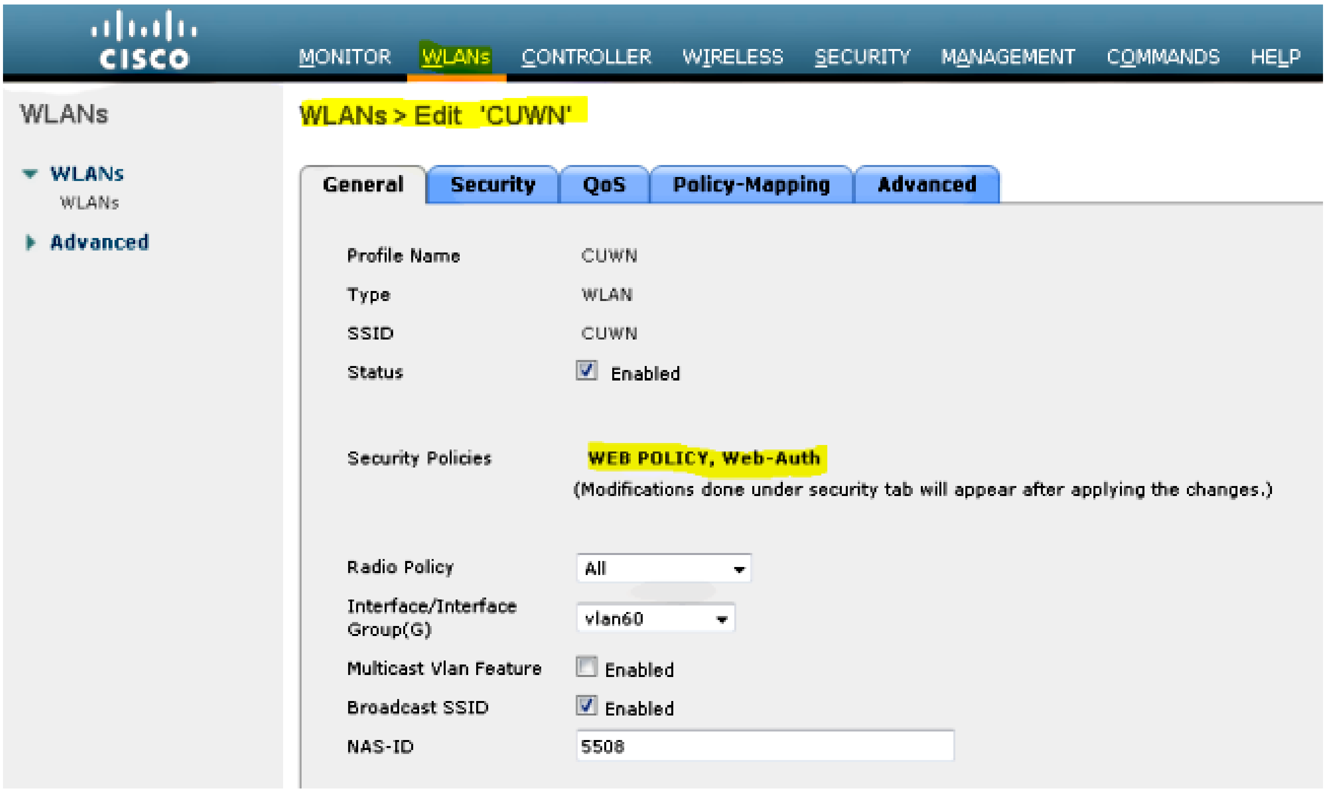
第1部分 — 5508锚点WLC上的配置

第2部分 — 5508/5760系列WLC和Catalyst 3850系列交换机之间的融合接入移动配置

第3部分 — 外部Catalyst 3850系列交换机的配置

第1部分 — 5508锚点WLC上的配置

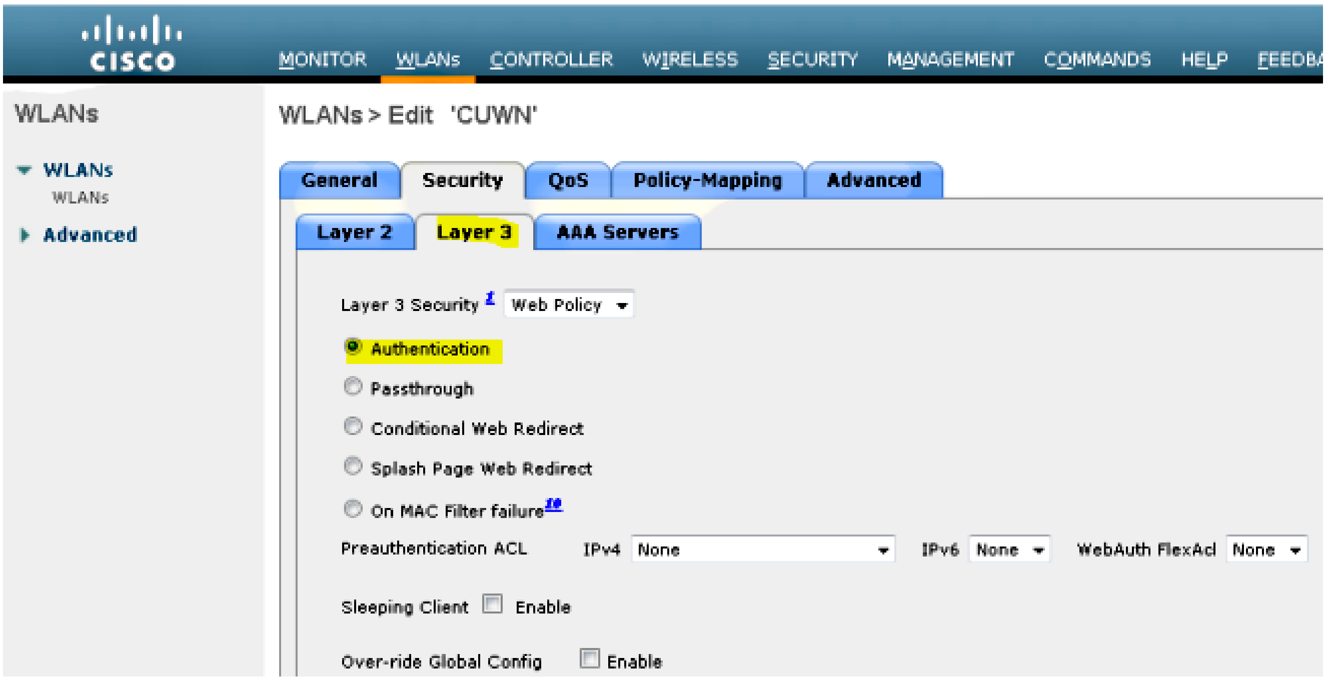
1. 在5508系列WLC上，将鼠标悬停在**WLAN > New**上，以便创建新的无线LAN(WLAN)。



WLANs > Edit 'CUWN'

Profile Name	CUWN
Type	WLAN
SSID	CUWN
Status	☑ Enabled
Security Policies	WEB POLICY, Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan60
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	5508

2. 将鼠标悬停在**WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication**上，以配置第3层安全。


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'CUWN'

Layer 3 Security Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

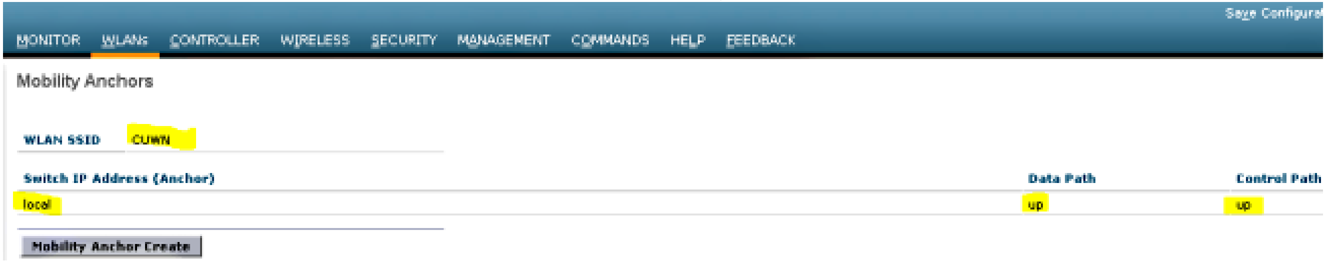
○ On MAC Filter failure

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

Sleeping Client □ Enable

Over-ride Global Config □ Enable

3. 在WLAN移动锚点配置窗口下将锚点地址**设为local**，以便将5508系列WLC添加为锚点。


Save Configura
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Mobility Anchor Create

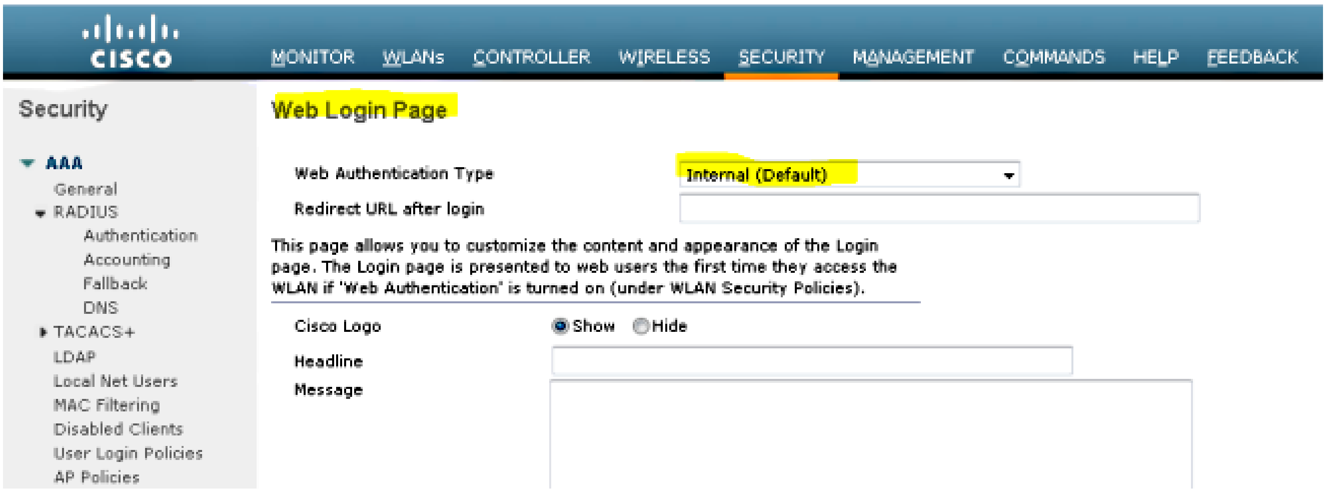
Mobility Anchors

WLAN SSID CUWN

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up

4. 将鼠标悬停在**Security > Webauth > Webauth page**上，以配置用于客户端身份验证的Webauth页。

   在本示例中，选择WLC Internal Webauth页面：



Web Login Page

Web Authentication Type Internal (Default)

Redirect URL after login

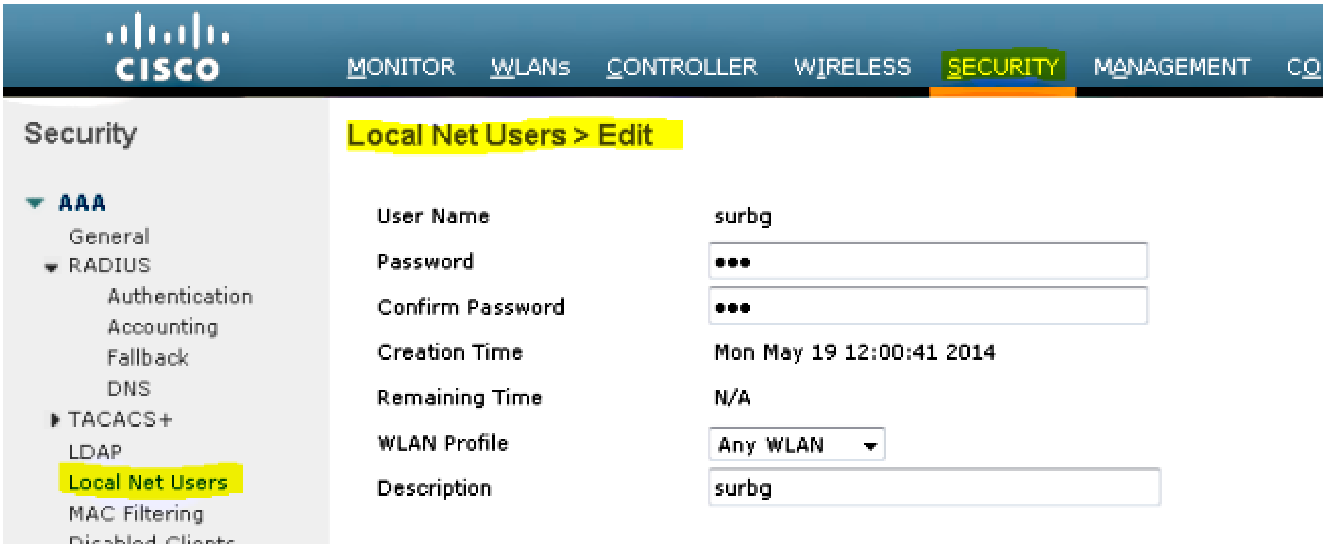
This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo ● Show ○ Hide

Headline

Message

5. 创建本地网络用户。在Webauth页面上出现提示时，用户将使用此用户名/密码对。

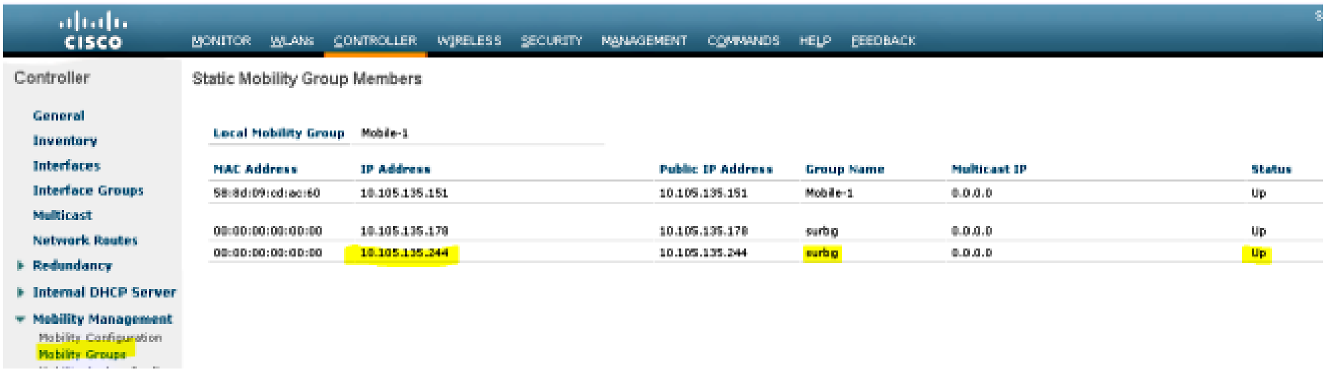


Local Net Users > Edit

User Name	surbg
Password	●●●
Confirm Password	●●●
Creation Time	Mon May 19 12:00:41 2014
Remaining Time	N/A
WLAN Profile	Any WLAN
Description	surbg

第2部分 — 5508/5760系列WLC和Catalyst 3850系列交换机之间的融合接入移动配置

1. 在5508系列WLC上，添加5760系列WLC作为移动对等体。

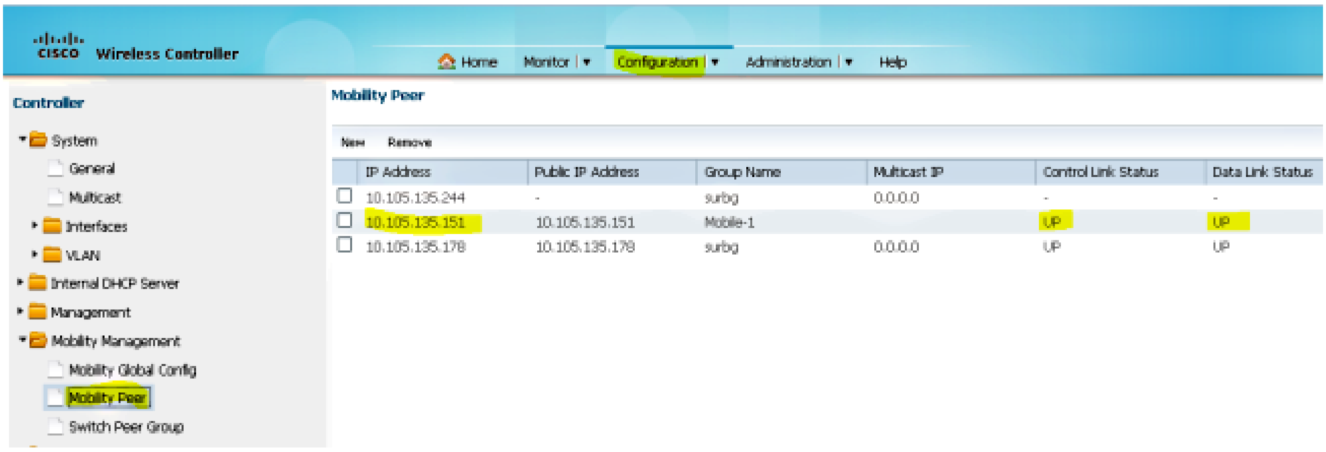


Static Mobility Group Members

Local Mobility Group Mobile-1

MAC Address	IP Address	Public IP Address	Group Name	Multicast IP	Status
58:8d:09:cd:ac:60	10.105.135.151	10.105.135.151	Mobile-1	0.0.0.0	Up
00:00:00:00:00:00	10.105.135.178	10.105.135.178	surbg	0.0.0.0	Up
00:00:00:00:00:00	10.105.135.244	10.105.135.244	surbg	0.0.0.0	Up

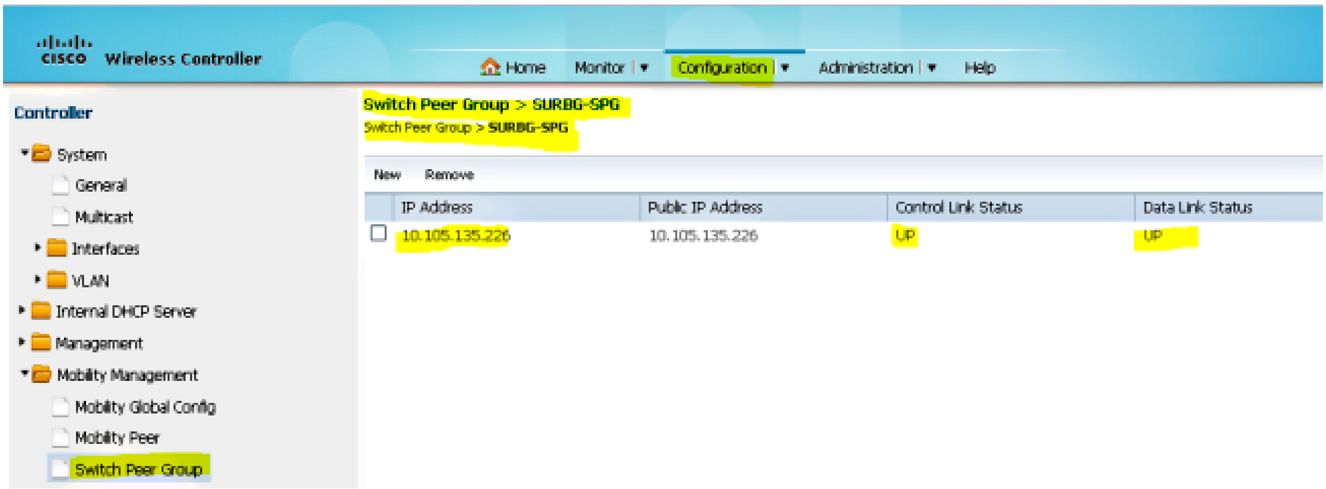
2. 在5760系列WLC上，作为移动控制器，添加5508系列WLC作为移动对等体。



Mobility Peer

	IP Address	Public IP Address	Group Name	Multicast IP	Control Link Status	Data Link Status
□	10.105.135.244	-	surbg	0.0.0.0	-	-
□	10.105.135.151	10.105.135.151	Mobile-1		UP	UP
□	10.105.135.178	10.105.135.178	surbg	0.0.0.0	UP	UP

3. 此步骤非常重要！将Catalyst 3850系列交换机作为5760系列WLC上的移动代理添加到Mobility Management下的Switch Peer Group选项卡下。

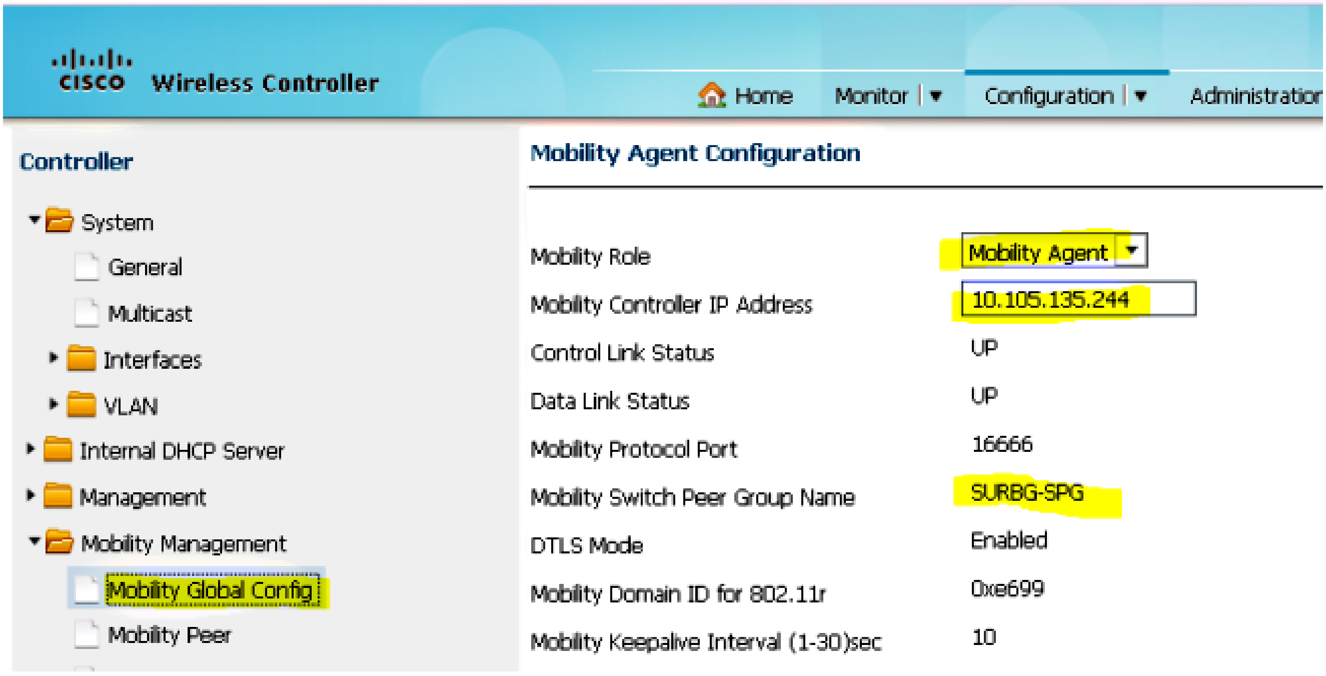


Switch Peer Group > SURBG-SPG

Switch Peer Group > SURBG-SPG

	IP Address	Public IP Address	Control Link Status	Data Link Status
□	10.105.135.226	10.105.135.226	UP	UP

4. 在Catalyst 3850系列交换机上，添加5760系列WLC作为移动控制器。执行此操作后，Catalyst 3850系列交换机将从移动控制器5760获取AP无法使用的许可证。

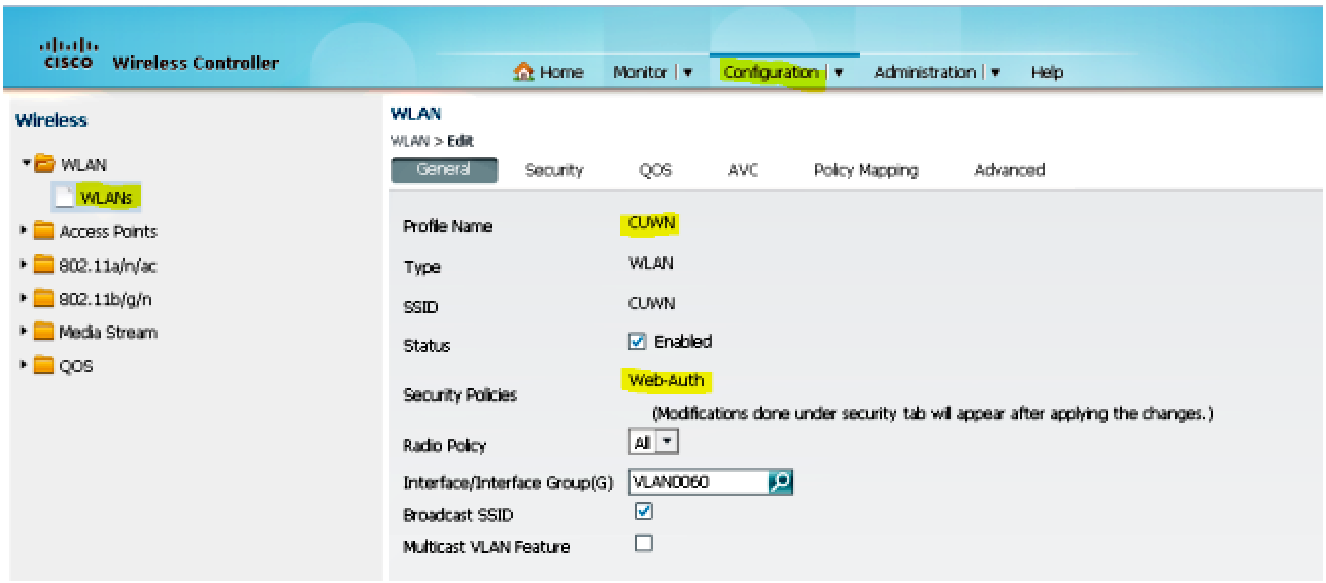


Mobility Agent Configuration

Mobility Role	Mobility Agent ▾
Mobility Controller IP Address	10.105.135.244
Control Link Status	UP
Data Link Status	UP
Mobility Protocol Port	16666
Mobility Switch Peer Group Name	SURBG-SPG
DTLS Mode	Enabled
Mobility Domain ID for 802.11r	0xe699
Mobility Keepalive Interval (1-30)sec	10

第3部分：外部Catalyst 3850系列交换机的配置

1. 将鼠标悬停在**GUI > Configuration > Wireless > WLAN > New**上，以便在Catalyst 3850系列交换机上配置确切的SSID/WLAN。

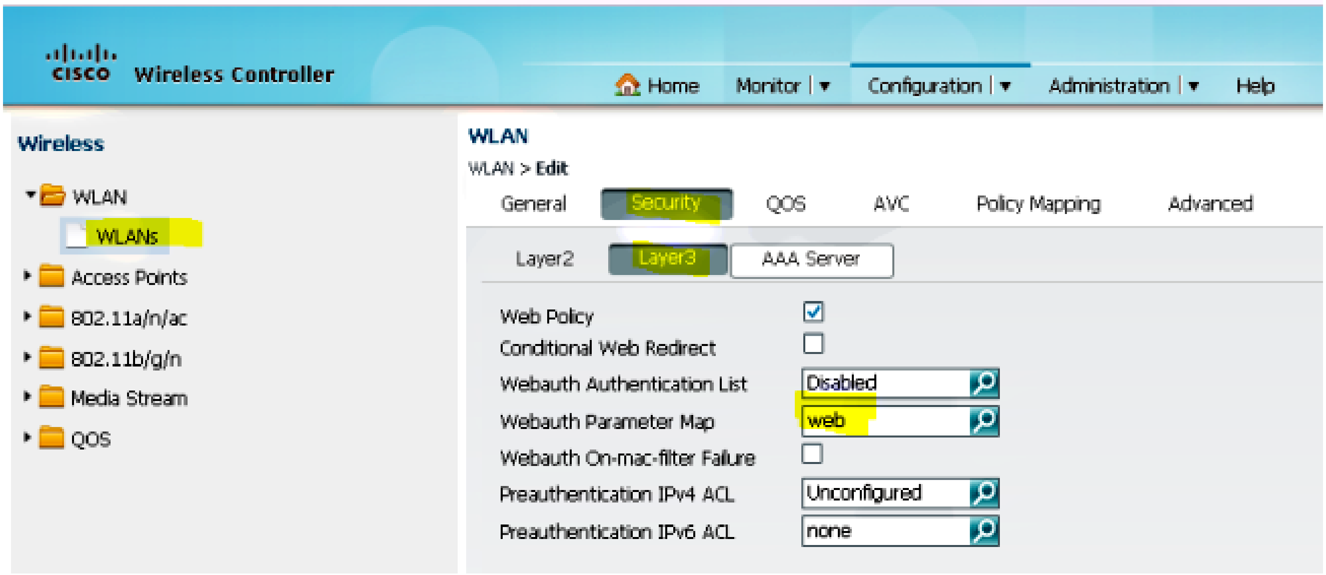


WLAN

WLAN > Edit

Profile Name	CUWN
Type	WLAN
SSID	CUWN
Status	☑ Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	VLAN0060
Broadcast SSID	☑
Multicast VLAN Feature	□

2. 将鼠标悬停在WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication上，以配置第3层安全。

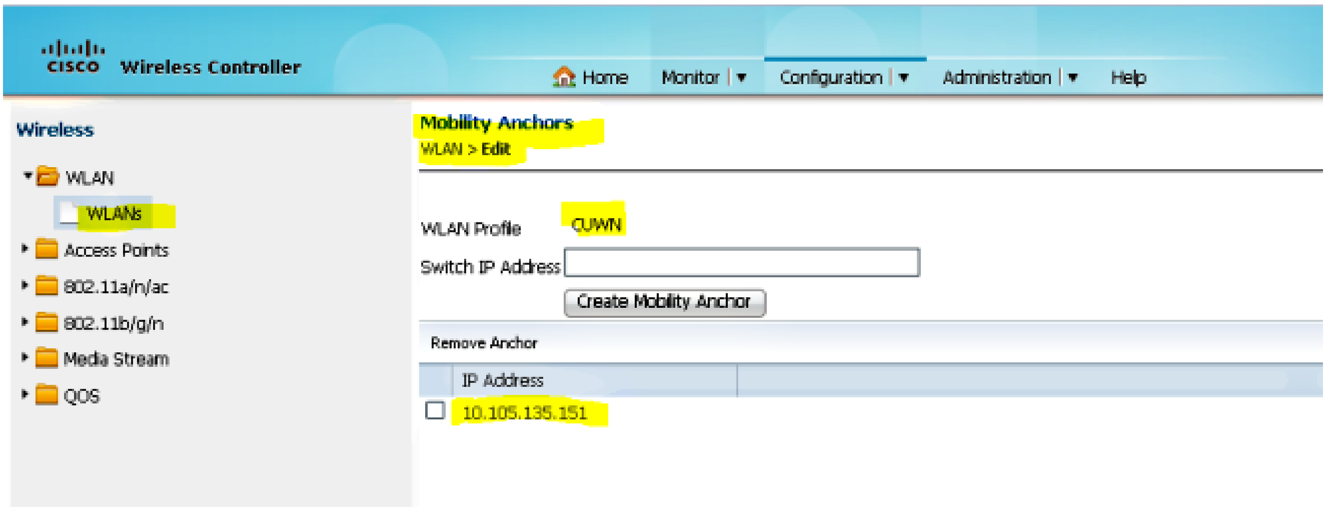


WLAN

WLAN > Edit

Web Policy	☑
Conditional Web Redirect	□
Webauth Authentication List	Disabled
Webauth Parameter Map	web
Webauth On-mac-filter Failure	□
Preauthentication IPv4 ACL	Unconfigured
Preauthentication IPv6 ACL	none

3. 将5508系列WLC IP地址添加为WLAN移动锚点配置下的锚点



Mobility Anchors

WLAN > Edit

WLAN Profile	CUWN
Switch IP Address	

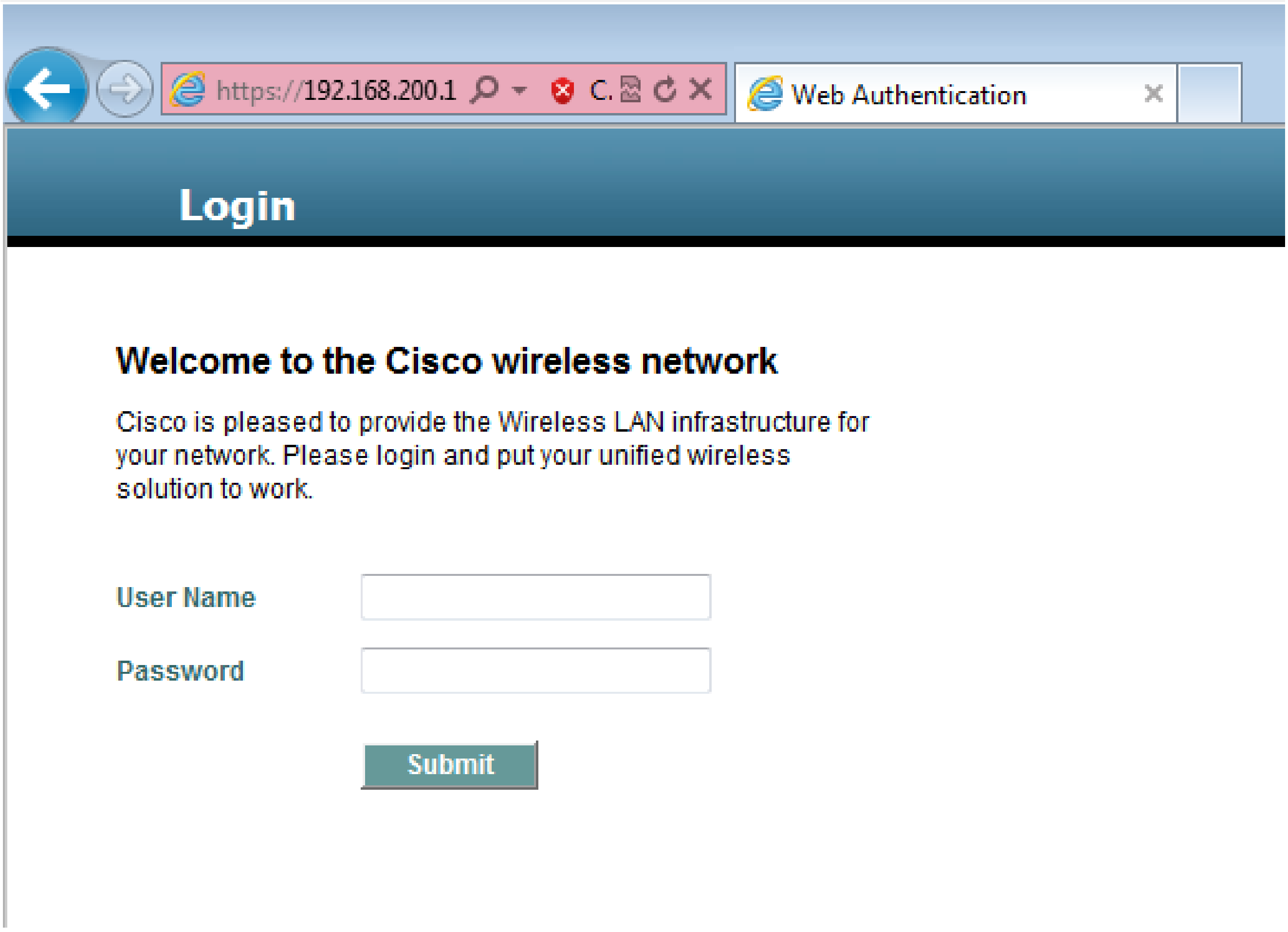
	IP Address
□	10.105.135.151

验证

使用本部分可确认配置能否正常运行。

将客户端连接到WLAN思科统一无线网络(CUWN)。工作流程如下：

1. 客户端收到IP地址。
2. 客户端打开浏览器并访问任何网站。
3. 客户端发送的第一个TCP数据包被WLC拦截，WLC拦截并发送Webauth页面。
4. 如果DNS配置正确，客户端将获得Webauth页面。
5. 客户端必须提供用户名/密码才能进行身份验证。
6. 身份验证成功后，客户端将重定向到原始访问页面。



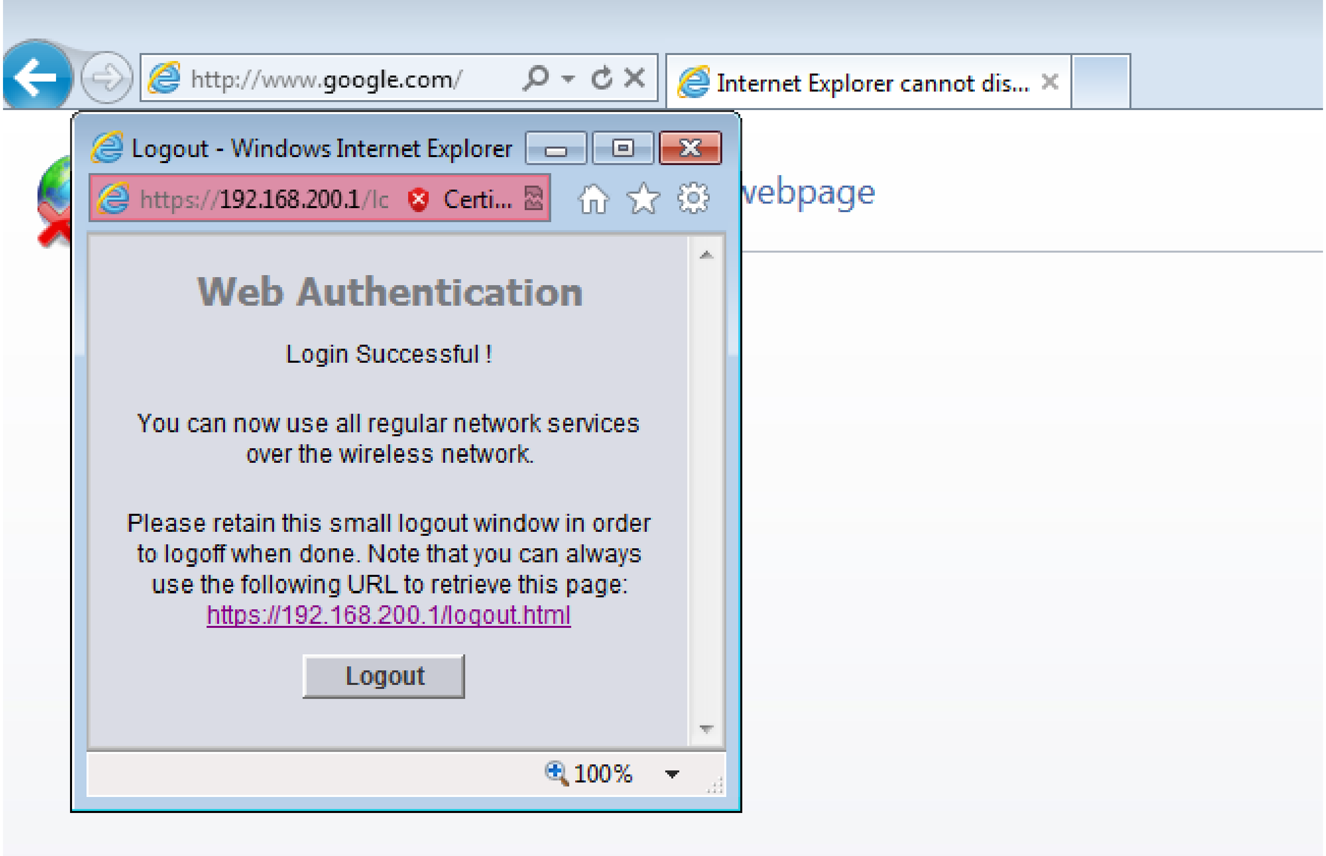
Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

7. 在客户端提供正确的凭证后，客户端将传递身份验证。



Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page:
https://192.168.200.1/logout.html

故障排除

要排除配置故障，请在5508系列WLC上输入以下调试，它充当访客锚点：

```
Debug Client
```

```
Debug web-auth redirect enable mac
```

示例如下：

```
Debug Client 00:17:7C:2F:B6:9A
Debug web-auth redirect enable mac 00:17:7C:2F:B6:9A

show debug

MAC Addr 1.................................. 00:17:7C:2F:B6:9A

Debug Flags Enabled:
 dhcp packet enabled.
 dot11 mobile enabled.
 dot11 state enabled
 dot1x events enabled.
 dot1x states enabled.
 FlexConnect ft enabled.
 pem events enabled.
 pem state enabled.
 CCKM client debug enabled.
 webauth redirect enabled.

*mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group,
marking intgrp NULL
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on
Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy
for client

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv4
ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2219)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv6
ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2240)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN
Policy over PMIPv6 Client Mobility Type
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an
intf for roamed client - removing intf group from mscb


*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4)
Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from
255 to 255

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl
from 65535 to 65535

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile
Station: (callerId: 53)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 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
 IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path
rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local Bridging Vlan = 60,
Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State
Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor,
client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Change state to DHCP_REQD (7) last state DHCP_REQD (7)

*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
```

```
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local
Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf
ID 13: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A ,
Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling mmSendIpv6AddrUpdate
for addition of IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , for MAC:
00:17:7C:2F:B6:9A
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800
Assigning an IPv6 Addr fe80:0000:0000:0000:6c1a:b253:d711:0c7f  to the client in
Anchor state update the foreign switch 10.105.135.226
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::
6c1a:b253:d711:c7f updated to mscb. Not Advancing pem state.Current state: mscb
in apfMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local Bridging
Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of
type 9, dtlFlags 0x4
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to
interface vlan60 which can support client subnet.
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7)
Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)

*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
pemAdvanceState2 6717, Adding TMP rule
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 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
 IPv4 ACL
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local Bridging
Vlan = 60, Local Bridging intf id = 13
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect rule
due to user logout
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148
Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign
switch 10.105.135.226
*dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11
to mobile
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for
```

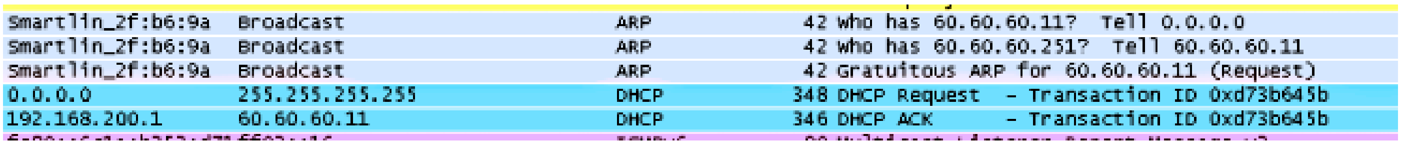
```
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU entry
of type 2, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6:
fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to
Data Plane. SUCCESS !!
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame

(5508-MC) >
(5508-MC) >
(5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received
op BOOTREQUEST (1) (len 314,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a 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
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 -
60.60.60.251 (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
REQUEST (3)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   op: BOOTREQUEST,
htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3
(2902502819), secs: 3072, flags: 0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   chaddr:
00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0,
yiaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0,
giaddr: 60.60.60.2
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   requested ip:
60.60.60.11
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to
60.60.60.251 (len 358, port 1, vlan 60)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 -
control block settings:
           dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
           dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2  VLAN: 60
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -
NONE (server address 0.0.0.0,local address 0.0.0.0, gateway 60.60.60.251, VLAN 60,
port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op BOOTREPLY
(2) (len 308,vlan 60, port 1, encap 0xec00)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server from ACK
(server 60.60.60.251, yiaddr 60.60.60.11)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   chaddr:
00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   server id:
192.168.200.1  rcvd server id: 60.60.60.251
*webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not
```

```
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a-  parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=,
URL is now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 312


*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is
 HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/
Content-Type: text/html
Content-Length: 312

<HTML><HEAD
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection

*emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a

*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL
according to configured Web-Auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a-  parser host is
www.facebook.com
```

```
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is
/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is
now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is
 HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
Content-Type: text/html
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op
BOOTREQUEST (1) (len 308,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
           dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0,
           dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2  VLAN: 60


*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1



*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:47.215:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_NOL3SEC
(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASTPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
  type = Airespace AP Client
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID =
```

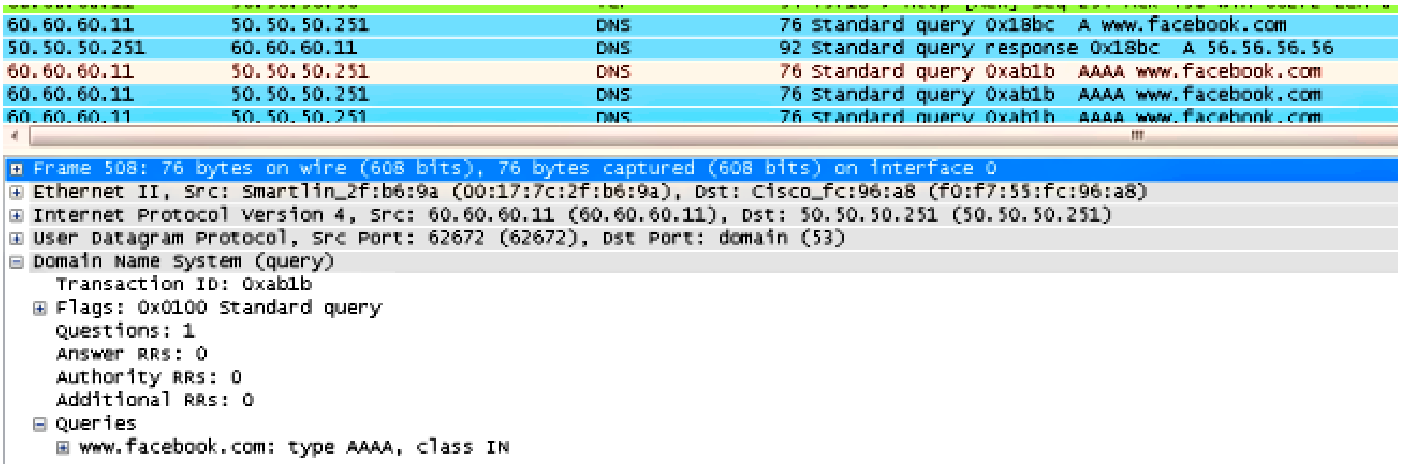
这是客户端数据包捕获。

客户端获取IP地址。



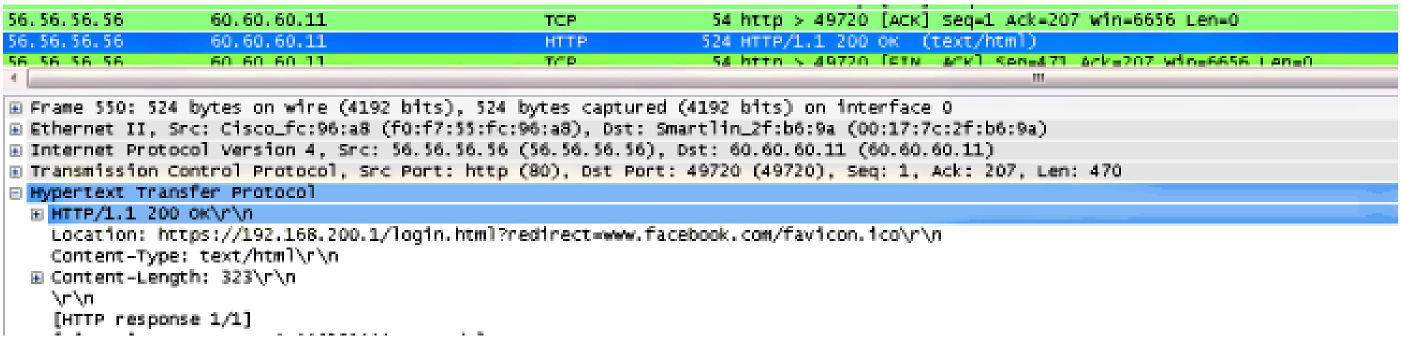
```
Smartlin_2f:b6:9a   Broadcast         ARP    42 Who has 60.60.60.11?  Tell 0.0.0.0
Smartlin_2f:b6:9a   Broadcast         ARP    42 Who has 60.60.60.251?  Tell 60.60.60.11
Smartlin_2f:b6:9a   Broadcast         ARP    42 Gratuitous ARP for 60.60.60.11 (Request)
0.0.0.0             255.255.255.255   DHCP  348 DHCP Request  - Transaction ID 0xd73b645b
192.168.200.1       60.60.60.11       DHCP  346 DHCP ACK      - Transaction ID 0xd73b645b
```

客户端打开浏览器并键入www.facebook.com。



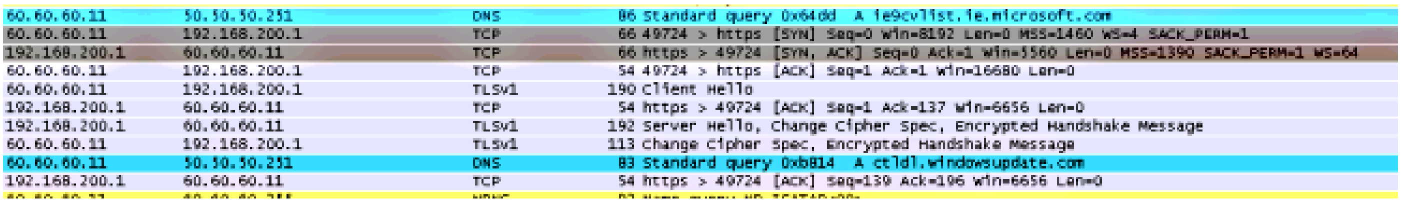
```
60.60.60.11     50.50.50.251    DNS    76 Standard query 0x18bc  A www.facebook.com
50.50.50.251    60.60.60.11     DNS    92 Standard query response 0x18bc  A 56.56.56.56
60.60.60.11     50.50.50.251    DNS    76 Standard query 0xab1b  AAAA www.facebook.com
60.60.60.11     50.50.50.251    DNS    76 Standard query 0xab1b  AAAA www.facebook.com
60.60.60.11     50.50.50.251    DNS    76 Standard query 0xab1b  AAAA www.facebook.com

⊞ Frame 508: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
⊞ Ethernet II, Src: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a), Dst: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8)
⊞ Internet Protocol Version 4, Src: 60.60.60.11 (60.60.60.11), Dst: 50.50.50.251 (50.50.50.251)
⊞ User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0xab1b
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ www.facebook.com: type AAAA, class IN
```

WLC会拦截客户端的第一个TCP数据包，并推送其虚拟IP地址和内部Webauth页面。



```
56.56.56.56    60.60.60.11    TCP     54 http > 49720 [ACK] Seq=1 Ack=207 Win=6656 Len=0
56.56.56.56    60.60.60.11    HTTP   524 HTTP/1.1 200 OK  (text/html)
56.56.56.56    60.60.60.11    TCP     54 http > 49720 [FIN, ACK] Seq=471 Ack=207 Win=6656 Len=0

⊞ Frame 550: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0
⊞ Ethernet II, Src: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8), Dst: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a)
⊞ Internet Protocol Version 4, Src: 56.56.56.56 (56.56.56.56), Dst: 60.60.60.11 (60.60.60.11)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49720 (49720), Seq: 1, Ack: 207, Len: 470
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico\r\n
    Content-Type: text/html\r\n
  ⊞ Content-Length: 323\r\n
    \r\n
    [HTTP response 1/1]
```

Web身份验证成功后，工作流的其余部分完成。



```
60.60.60.11      50.50.50.251     DNS      86 Standard query 0x64dd  A ie9cvlist.ie.microsoft.com
60.60.60.11      192.168.200.1    TCP      66 49724 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
192.168.200.1    60.60.60.11      TCP      66 https > 49724 [SYN, ACK] Seq=0 Ack=1 Win=5560 Len=0 MSS=1390 SACK_PERM=1 WS=64
60.60.60.11      192.168.200.1    TCP      54 49724 > https [ACK] Seq=1 Ack=1 Win=16680 Len=0
60.60.60.11      192.168.200.1    TLSv1   190 Client Hello
192.168.200.1    60.60.60.11      TCP      54 https > 49724 [ACK] Seq=1 Ack=137 Win=6656 Len=0
192.168.200.1    60.60.60.11      TLSv1   192 Server Hello, Change Cipher Spec, Encrypted Handshake Message
60.60.60.11      192.168.200.1    TLSv1   113 Change Cipher Spec, Encrypted Handshake Message
60.60.60.11      50.50.50.251     DNS      83 Standard query 0xb814  A ctldl.windowsupdate.com
192.168.200.1    60.60.60.11      TCP      54 https > 49724 [ACK] Seq=139 Ack=196 Win=6656 Len=0
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。