Cisco Catalyst 6500 Series

Wireless LAN Services Module (WLSM) Deployment Guide

August 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6274-01
CONTENTS

Layer 3 Mobility Overview 1
  mGRE Tunnels 2
  WDS 2

Configuration Overview 3
  Verify Hardware and Software 3
    Hardware Components 3
    Software Components 4
  Configure Communications between the Supervisor 720 and WLSM 4
  Configure mGRE Tunnels on the Supervisor 720 6
  Configure the RADIUS Server for LEAP Authentication 9
  Configure the WDS on the WLSM 11
    Configure Communications from the WDS to the RADIUS Server 11
    Configure Pass-Through Client Authentication 11
  Configure an Access Point 12
    Register with the WDS 12
    Link SSIDs with Mobility Tunnels – Single Encryption Scheme 14
    Link SSIDs with Mobility Tunnels – Multiple Encryption Schemes 17

Additional Considerations 21
  IP Addressing for Mobile Clients 21
  Fast Secure Roaming 22
  IP Multicast 23
  Fragmentation 23

Configure the WLSE for WDS 24

Configurations 27
  WLSM Configuration 27
  Supervisor 720 Configuration 28
  Access Point Configuration – Single Encryption Scheme 30
  Access Point Configuration – Multiple Encryption Scheme 31
  Configuration Map 35
Layer 3 Mobility Overview

Mobility in a wireless LAN environment can present a challenge as the physical reach of the network grows. Applications such as voice require sub-150 ms roam times and expect IP address continuity regardless of the Layer 3 boundaries that are crossed. Deploying a sprawling Layer 2 network can subject user traffic to delays and loss of service due to issues such as broadcast storms and Spanning Tree Protocol (STP) reconvergence times.

Layer 3 mobility provides a better performing and more scalable approach. Access points may be deployed in any location in a large Layer 3 network without requiring a single VLAN to be carried throughout the wired switch infrastructure. An overlay of multipoint GRE (mGRE) tunnels allows clients to roam to other access points residing on different Layer 3 subnets without loss of connectivity or a change in IP addressing.

The Cisco Structured Wireless-Aware Network (SWAN) Layer 3 mobility solution consists of various hardware and software components. For more information about SWAN, go to Cisco.com:

http://www.cisco.com/go/swan

The three primary devices are as follows:

- Cisco Aironet 1100 and 1200 Series Access Points
- Catalyst 6500 (and its Supervisor 720 Module)
- Catalyst 6500 Series Wireless LAN Services Module (WLSM)

The software component that provides coordination between these devices and the mobile nodes using its services is called the Wireless Domain Services (WDS). The WDS runs on the WLSM. Each of these components must be configured to work together as a unified system.

Configuring Layer 3 mobility requires linkage between different hardware and software components, and is best accomplished by separating the functional components into modules, configuring each module individually, and verifying that each module works properly before proceeding to the next.

Figure 1 provides an overview of components that make up the Layer 3 mobility solution.
Layer 3 Mobility Overview

mGRE Tunnels

The “plumbing” that enables Layer 3 mobility consists of Multipoint Generic Routing Encapsulation (mGRE) tunnels. Each tunnel has a single termination point on the Supervisor 720 module of the Catalyst 6500 that hosts the WLSM. The other logical endpoint of the tunnel exists on all access points participating in the Layer 3 mobility network. Clients that associate to a participating access point associate to a particular SSID. The SSID is mapped to a mobility network that tunnels all client traffic to the Catalyst 6500. The Supervisor 720 maintains a database of the clients (mobile nodes) and the access points to which they are associated. Roaming from one access point to another simply requires updating the database and changing the forwarding information for that mobile node.

WDS

The WDS software provides a control mechanism for wireless clients that roam between access points residing on different layer 3 subnets.

When WDS is in the WLSM, the access points providing Layer 3 mobility must register with the WDS before wireless clients are given access to the mobility network. The location of the WDS is specified in each access point along with LEAP device credentials that are required for authentication with the WDS. Once the access point is authenticated, it is considered registered. A registered access point is provided with the information needed to build mGRE tunnels to the Supervisor module in the Catalyst 6500.
Configuration Overview

Setting up Layer 3 mobility consists of six basic steps:
1. Verify hardware and software
2. Configure communications between the Supervisor 720 and the WLSM
3. Configure mGRE tunnels on the Supervisor 720
4. Configure the RADIUS server for LEAP authentication
5. Configure the WDS on the WLSM
6. Configure an access point

Verify Hardware and Software

Before configuring Layer 3 mobility, be sure to verify proper operation of the hardware components and ensure that all equipment is running at the appropriate revisions of software including the following:
- Supervisor 720
- WLSM
- Access points
- CiscoSecure ACS server
- CiscoWorks WLSE

Hardware Components

The Catalyst 6500 that houses the WLSM must use the Supervisor 720 module. Note that all Catalyst 6500 chassis except the Catalyst 6503 require the fan tray 2 module, which in turn requires the 2500W power supply for proper operation. For planning purposes, be aware that the 2500W power supplies use a 20 amp circuit with a NEMA plug.

In the current configuration, the WLSM module is present in slot 1. Before proceeding with any configuration, ensure that the module is recognized. The Status LED should be solid green. If the LED is not solid green, the Supervisor 720 may not be running a version of code that recognizes the WLSM, or there may be a hardware problem with the module. In the show module display below, note that the WLSM module in slot 1 is recognized by the Supervisor module and has passed diagnostics.

```
Sup720...#show module

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Wireless LAN Service Module</td>
<td>WS-SVC-WLAN-1-K9</td>
<td>SAD0805032J</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>8 port 1000mb GBIC Enhanced QoS</td>
<td>WS-X6408A-GBIC</td>
<td>SAL05073UXR</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
<td>48 port 10/100 mb RJ45</td>
<td>WS-X6348-RJ-45</td>
<td>SAD05090C87</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>Supervisor Engine 720 (Active)</td>
<td>WS-SUP720-BASE</td>
<td>SAD0802089E</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod MAC addresses</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0003.feae.3388 to 0003.feae.338f</td>
<td>3.0</td>
<td>7.2(1)</td>
<td>1.1(1)</td>
<td>Ok</td>
</tr>
<tr>
<td>0002.fc45.e480 to 0002.fc45.e487</td>
<td>2.0</td>
<td>5.4(2)</td>
<td>8.3(0.156)</td>
<td>RO Ok</td>
</tr>
<tr>
<td>0002.fc26.ea24 to 0002.fc26.ea53</td>
<td>2.0</td>
<td>5.4(2)</td>
<td>8.3(0.156)</td>
<td>RO Ok</td>
</tr>
<tr>
<td>000d.6535.ff20 to 000d.6535.ff23</td>
<td>3.0</td>
<td>7.7(1)</td>
<td>12.2(ROCKIES)</td>
<td>Ok</td>
</tr>
</tbody>
</table>
```
Software Components

The minimum software revisions for Layer 3 mobility support are listed in Table 1. However, Cisco recommends using the most current software releases.

Some screen captures in this document reflect pre-release versions of software.

Table 1 Minimum Software Revisions for Layer 3 Mobility Support

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor 720</td>
<td>IOS version 12.2(18)SXD</td>
</tr>
<tr>
<td>WLSM</td>
<td>Version 1.1(1)</td>
</tr>
<tr>
<td>Access points</td>
<td>IOS version 12.2(15)XR</td>
</tr>
<tr>
<td>CiscoSecure ACS server</td>
<td>Version 2.6 (for LEAP support)</td>
</tr>
<tr>
<td>CiscoWorks WLSE</td>
<td>Version 2.7.1</td>
</tr>
</tbody>
</table>

Configure Communications between the Supervisor 720 and WLSM

The WLSM and the Supervisor 720 must define a common VLAN used to communicate with the outside world. Once the VLAN is configured and tested, enable Layer 3 mobility as shown in the following Cisco IOS scripts:

**On the Supervisor 720:**

```
! --Create the VLAN shared by the WLSM and the Supervisor 720.
Sup720...(config)# vlan 100

! --Configure the VLAN interface.
Sup720...(config)# interface Vlan100

! --Assign an appropriate IP address and subnet mask for VLAN 100
Sup720...(config-if)# ip address 10.0.100.1 255.255.255.0
Sup720...(config-if)# exit

! --Specify that this VLAN should be used to communicate with the WLSM (residing in slot 1 in this particular chassis)
Sup720...(config)# wlan module 1 allowed-vlan 100
```
On the WLSM:

WLSM...# config t
! --Create a VLAN that will be shared by the WLSM and Supervisor 720
WLSM...(config)# wlan vlan 100
!
! --Assign a unique IP address and appropriate subnet mask
WLSM...(config-vlan)# ipaddr 10.0.100.2 255.255.255.0
!
! --Define a default gateway used to direct the WLSM's traffic to the
! --Supervisor module by providing the Supervisor's IP address on this
! --VLAN as the WLSM's Gateway
WLSM...(config-vlan)# gateway 10.0.100.1
!
! --Specify "admin" for this VLAN to turn on L3 Mobility and start the WDS
! --process
WLSM...(config-vlan)# admin

The following show command indicates that the Supervisor 720 module is communicating with the WLSM module.

Sup720...#show mobility wlan-module
Number of Wireless Access Modules : 1
WAM currently in use : 1
 In Use : 1
 Refresh Retries : 0
 Refresh Timer : 0x44BC7828
 Last sent global Message ID : 105
 Last sent global Message ID to this slot 0
 Comm. status with slot 1 : up

From the WLSM, LCP link status should be up and the WDS process should be ACTIVE:

WLSM...#sh wlc pl status
 MAC: 0060.2f30.a85b, IP-ADDR: 10.0.100.2
 State: Administratively StandAlone - ACTIVE
 AP Count: 3 , MN Count: 2
 LCP link status: up
 HSRP state: Not Applicable
WLSM...#

With both modules configured, test the connection between the two devices.

From the WLSM to the Supervisor 720:

WLSM...#ping 10.0.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

From the Supervisor 720 to the WLSM:

Sup720...#ping 10.0.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Sup720...#
Configure mGRE Tunnels on the Supervisor 720

One mGRE tunnel must be defined on the Supervisor 720 module for each mobility group. A mobility group is a group of wireless clients that are grouped together for some shared characteristic such as a common authentication or encryption scheme, or service such as VoIP, or user types such as visitors and employees. Settings defined within the tunnel are dynamically pushed to the access points participating in Layer 3 mobility.

The following configuration illustrates a single tunnel setup using the arbitrary tunnel number 100:

```
! --Begin by defining a unique loopback interface for each tunnel.
! --It is important to note that each tunnel requires its own loopback
! --interface.
Sup720...(config)# interface Loopback100
!
! --Assign an IP address and subnet mask to be used as the tunnel’s
! --source address. Note that this is different from the addresses that will
! --be assigned to wireless clients and to the tunnel.
Sup720...(config-if)# ip address 10.80.0.1 255.255.255.255
!
! --Define the tunnel interface
Sup720...(config-if)# interface Tunnel100
!
! --Assign an IP Address and subnet mask appropriate to the tunnel.
! --This address will be used as the default gateway for wireless
! --clients on this L3 Mobility network.
Sup720...(config-if)# ip address 172.16.1.1 255.255.255.0
!
! --Tie the tunnel to the loopback interface.
Sup720...(config-if)# tunnel source Loopback100
!
! --Enable mGRE on this tunnel
Sup720...(config-if)# tunnel mode gre multipoint
!
! --The mobility network-id defines this as a unique mobility network.
! --The network-id defined for this tunnel will also be defined under one of
! --the access point’s SSID definitions to identify its participation in this
! --Layer 3 Mobility network.
mobility network-id 100

The tunnel is now defined and additional items can be configured on the tunnel interface, which include:

```
interface Tunnel100
!
! --Use a descriptor to identify the type of clients in this tunnel
description LEAP_wireless_clients
!
! --IP Redirects should be disabled (and are disabled by default, so this
! --command is only necessary if that default behavior has been changed).
no ip redirects
!
! --By default, a mobility network is considered “untrusted”. In an untrusted
! --network, mobile nodes are required to use a DHCP-obtained IP address.
! --In a “trusted” network, mobile nodes are allowed to use static IP
! --addresses. The following command allows static IP addressing:
 mobility trust
!
! --Enable DHCP packet snooping. This feature is used by the Supervisor 720
! --module to populate the IP addresses of mobile clients in the Forwarding
! --Information Base when the network is considered “untrusted”. (Trusted
```
! --networks obtain IP addressing by snooping IP packets generated by a
! --mobile node). Note that the corresponding global command “ip dhcp
! --snooping” is also required when using an untrusted network.
ip dhcp snooping packets
!
!
! --By default, broadcasts are received, but not forwarded on a tunnel
! --interface. This behavior can be enabled on a per-tunnel basis.
mobility broadcast
!
!
! --If a mobility network uses a DHCP server that is not resident on
! --the Supervisor 720, configure a helper-address to convert the
! --DHCP requests from broadcast to unicast directed to the DHCP server.
ip helper-address 10.91.104.76

The mobility network-id used on the tunnel interface must be unique for each mobility group. A mobility group consists of a mobility network ID, an SSID, and optionally, some type of security (authentication and encryption). Having properly configured the tunnel interface, use the show interface tunnel 100 command to ensure that it is up and operational as shown below.

Sup720...#show interface tunnel 100
Tunnel100 is up, line protocol is up
   Hardware is Tunnel
   Description: To_wireless_clients
   Internet address is 172.16.1.1/24
   MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation TUNNEL, loopback not set
   Keepalive not set
   Tunnel source 10.80.0.1 (Loopback100), fastswitch TTL 255
   Tunnel protocol/transport multi-GRE/IP, key disabled, sequencing disabled
   Checksumming of packets disabled, fast tunneling enabled
   Last input 00:00:00, output 00:00:00, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue: 0/0 (size/max)
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
   L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
   L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
   178707 packets input, 19823493 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   102869 packets output, 10834504 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out

Verify that the mobility network is up and running with the correct parameters.

Sup720...#show mobility network 100
Wireless Network ID : 100
Wireless Tunnel Source IP Address : 10.80.0.1
Wireless Network Attributes : Trusted, Broadcast Enabled
Wireless Network State : Up

Registered Access Point on Wireless Network 100:
 AP IP Address     AP Mac Address     Wireless Network-ID
                    -----------          ---------------
                     10.10.0.29     0005.9a39.aeba  100 0
Registered Mobile Nodes on Wireless Network 100:

<table>
<thead>
<tr>
<th>MN Mac Address</th>
<th>MN IP Address</th>
<th>AP IP Address</th>
<th>Wireless Network-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0006.d786.3842</td>
<td>172.16.1.24</td>
<td>10.10.0.29</td>
<td>100</td>
</tr>
</tbody>
</table>

Sup720...#

For a global view of all tunnels configured on this Supervisor module, use the `show mobility` command:

```
Sup720...#show mobility status

WLAN Module is located in Slot: 1 (HSRP State: Not Applicable)
LCP Communication status : up
MAC address used for Proxy ARP: 0005.5f54.5800
Number of Wireless Tunnels : 2
Number of Access Points : 1
Number of Mobile Nodes : 1

Wireless Tunnel Bindings:

<table>
<thead>
<tr>
<th>Src IP Address</th>
<th>Wireless Network-ID</th>
<th>Trusted</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.80.0.1</td>
<td>100</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>10.80.0.2</td>
<td>101</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Important:** Through your routing protocol of choice, ensure that the loopback addresses and internal tunnel addresses (addresses that will be assigned to clients within the tunnel) are routable. In our example configuration, EIGRP is the routing protocol. The loopback addresses are advertised using the `redistribute connected` command. The tunnel addresses are specified using the `network` command.

```
! router eigrp 100
    redistribute connected
    network 10.91.104.0 0.0.0.255
    network 172.16.0.0
    auto-summary
    
! The routing table that should reflect routes for the networks/interfaces used and should advertise them so that other devices will know how to reach them and the tunnels that they represent.
```

```
Sup720...#show ip route

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
 D  172.16.0.0/16 is a summary, 6d18h, Null0
 C  172.16.1.0/24 is directly connected, Tunnel100
 C  172.16.2.0/24 is directly connected, Tunnel101
 D  10.0.0.0/8 is a summary, 6d18h, Null0
 D  10.18.0.0/24 [90/28416] via 10.91.104.69, 21:21:59, Vlan1
 D  10.19.0.0/24 [90/28416] via 10.91.104.69, 21:22:02, Vlan1
 D  10.16.0.0/24 [90/28416] via 10.91.104.69, 21:22:02, Vlan1
 D  10.17.0.0/24 [90/28416] via 10.91.104.69, 21:22:02, Vlan1
 D  10.50.10.0/24 [90/281856] via 10.91.104.90, 6d18h, Vlan1
 D  10.91.96.100/30 [90/3072] via 10.91.104.65, 6d18h, Vlan1
 C  10.80.0.2/32 is directly connected, Loopback101
 C  10.80.0.1/32 is directly connected, Loopback100
 C  10.80.0.2/32 is directly connected, Loopback100
 C  10.80.0.2/32 is directly connected, Loopback100
 S* 0.0.0.0/0 [1/0] via 10.91.104.65
```

Cisco recommends that the tunnel interfaces be configured as passive interfaces so as not to propagate unnecessary routing traffic over the tunnels (such as passive-interface tunnel100).
Configure the RADIUS Server for LEAP Authentication

In the Cisco Structured Wireless-Aware Network (SWAN) framework, infrastructure devices (access points) and the WLSE establish secure communications with the WDS using LEAP authentication. Before access points and the WLSE can authenticate to the WDS, the CiscoSecure ACS server or third-party LEAP-compliant server (such as Funk Software or Interlink) must be configured.

The WLSM must be defined on the RADIUS server as an AAA Client, which allows the WLSM to make requests to authenticate the LEAP credentials of registering devices. Using the CiscoSecure ACS RADIUS server, select Network Configuration, define the IP address of the WDS and the shared RADIUS key, and specify Radius (Cisco Aironet) as the authentication type as shown in Figure 2.

![Figure 2 Defining the WDS on the AAA Server](image)

Devices such as access points that participate in Layer 3 mobility must have their LEAP credentials defined on the RADIUS server as shown in Figure 3. Configure each device by selecting the User Setup tab. Define the name for the device (as specified on the access point or WLSE) and specify that this user’s authentication credentials must be checked against the CiscoSecure database. Complete the entry by configuring the password for this user. You can use this entry for a single access point or for a number of access points in the network.
Troubleshooting authentication problems may require the use of the Reports and Activity log on the ACS server. Check the passed attempts (Figure 4) and failed attempts (Figure 5) for requests being sourced by the WDS (which appear as the NAS on the ACS server).
Configure the WDS on the WLSM

Configure Communications from the WDS to the RADIUS Server

Configuring the WDS to communicate with the RADIUS requires the following steps detailed in a `show run` command:

```
aaa new-model
!
! --Define a group used to authenticate LEAP devices
aaa authentication login leap-devices group radius
!
! --Define the RADIUS server used to LEAP-authenticate devices
radius-server host 10.91.104.76 auth-port 1645 acct-port 1646
radius-server key cisco
!
! --Configure the WDS to use the defined authentication group
wlccp authentication-server infrastructure leap-devices
```

Configure Pass-Through Client Authentication

Access points registered with a WDS no longer communicate directly with a RADIUS server to authenticate 802.1X wireless clients. Once an access point registers with the WDS, it funnels all subsequent registrations through the WDS whether they are infrastructure authentications performed as part of the device's WDS re-registration or client authentications performed as part of a client’s association to the access point.

The WDS must be configured to pass client authentications through to a RADIUS server. Without this configuration, client authentications will fail and clients will be unable to associate to the access point.
The following script shows how to configure the WLSM running the WDS to enable client authentication pass-thru:

```
! aaa new-model
! --Define a group used to authenticate client devices
! aaa authentication login client-authentication group radius
! --Define the RADIUS server used for the client group
! radius-server host 10.91.104.76 auth-port 1645 acct-port 1646
! radius-server key cisco
! --Point the AP to the AAA group used for client authentication
! wlccp authentication-server client any client-authentication
! --Note that the client authentication can be configured for specific
! --802.1x authentication types by replacing "any" with the desired
! --authentication type
```

Authentication messages flow from the access point to the WDS and from the WDS to the RADIUS server. The RADIUS server approves or rejects the device credentials and replies to the WDS. The WDS will pass the RADIUS server’s reply to the access point. When debugging, check that each step in the process completes without failure. On the WDS, run one or more of the following debugs to assist in troubleshooting client authentication through the WDS:

```
WLSM...#debug wlccp wds ?
aggregator     Radio measurement(rm) aggregator
authenticator  MAC and EAP authenticator
mobility       Layer-3-Mobility
nm             Network Management
state          WDS fsm state transitions
statistics     WDS statistics
```

### Configure an Access Point

#### Register with the WDS

The first configuration task on an access point is to enter LEAP credentials so that it can register with the WDS. Access points can be configured through the access point’s web-based interface, the access point’s CLI, or through a WLSE configuration job. The web interface and CLI are detailed here. For details on configuring access points using WLSE, refer to the following link:


Follow these steps to register an access point with the WDS:

**Step 1** Login to the access point web-based interface and navigate to the Wireless Services Table of Contents (TOC) item.

**Step 2** Select AP.

**Step 3** Select Enable.

**Note** Unlike an access point-based WDS that supports a Layer 2 discovery method, the WLSM-based WDS requires the access points to manually define the location of the WDS.
Step 4 Select the **Specified Discovery** radio button and enter the IP address of the WDS.

Step 5 Enter the username and password used to authenticate the infrastructure access point to the WDS.

### Note
The username and password can be a unique pair assigned to this access point, or a shared username/password pair used by a number of access points. In either case, be sure the credentials are configured on the RADIUS server that the WDS uses for its authentication.

Step 6 Select the **Enable** radio button to allow this access point to participate in L3 mobility.

Step 7 Click **Apply** to commit the configuration.

Figure 6 illustrates the configuration parameters.

**Figure 6  Access Point—Participating in Cisco SWAN**

To configure the same items through the Cisco IOS command line interface, enter the following commands:

```
! --Enter the LEAP credentials
wlccp ap username cisco password 7 14141B180F0B
! --Specify the IP address of the WDS
wlccp ap wds ip address 10.0.100.2
```

The access point attempts to register with the WDS. **Figure 8** shows a properly registered access point.
Figure 7  Access Point—Registered With WDS WLSM-7.BMP

The WDS portion of the access point configuration is complete.

Link SSIDs with Mobility Tunnels – Single Encryption Scheme

In order for mobile clients to associate to an access point, become registered mobile nodes, obtain an appropriate IP address, and be allowed to pass traffic on a Layer 3 mobility tunnel, linkage must be made between the RF-side (SSID) and the tunnel-side (mobility network-id). Specifying the **mobility network-id** as part of the SSID definition places all traffic from clients associated to that SSID into the corresponding tunnel.

The simplest of configurations involves a single SSID with open authentication and no encryption as shown in Figure 8 and Figure 9.

Figure 8  Access Point—Open Authentication SSID With Mobility Network ID
The Network ID in Figure 8 specifies the mobility network that maps to this newly-defined SSID. The following script shows the IOS configuration process:

```plaintext
! interface Dot11Radio0
  no ip address
  no ip route-cache
  ssid seagle-open
    authentication open
    mobility network-id 100
!
```

Rather than being open, an SSID could be configured for some form of authentication and encryption as shown in Figure 10 and Figure 11.
The script below shows the Cisco IOS configuration process:

interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers ckip
!
ssid seagle-leap
  authentication open eap eap_method
  authentication network-eap eap_methods
  mobility network-id 101
!

Once configured, a client attempting to associate to the defined SSID is authenticated and added to the mobility group. To check for a successful client association, use the `show` command:

```
Seagle_ap1# show wlccp ap mobility forwarding
Wireless Control(0005.5f54.5800) IPv4 Forwarding Table
MAC Address    IP address    Tunnel address
0002.8aa3.24c0 172.16.1.22   10.80.0.1
```

On the Supervisor 720, check for registered mobile nodes:

```
Sup720...#show mobility mn
MN Mac Address  MN IP Address  AP IP Address  Wireless Network-ID
----------------- ----------------- --------------- -------------------
0002.8aa3.24c0   172.16.1.22   172.16.1.108      100
```

Additional SSIDs may be added to this radio’s configuration but, because encryption is defined under the radio interface and not under the individual SSIDs, they must all use the same encryption scheme. To configure multiple mobility groups using different encryption schemes requires the configuration of VLANs on the access point. These VLANs are only locally significant, meaning the Fast Ethernet side of the access point does not need to be configured as an 802.1q trunk (unless there is a need to configure more than one locally bridged VLAN as in the case of IP multicast traffic).
Link SSIDs with Mobility Tunnels – Multiple Encryption Schemes

In order to support multiple encryption schemes for multiple mobility networks on the access point, VLANs must be configured. However, these VLANs are only locally significant and are not trunked to the attached Ethernet switch. Configuring this arrangement on the CLI can be error-prone since many line items must be duplicated on both the radio interfaces and the Fast Ethernet interfaces. Cisco recommends that you perform the configuration using the GUI. When the configuration is complete, use the CLI to view it.

In the sample configuration, since the native VLAN is the only defined VLAN that is not tied to a mobility network-id, the upstream switch does not need to be configured as a trunk. The VLAN definitions are made solely for the convenience of creating mobility groups with separate encryption schemes and therefore do not need to trunked. If more than one defined VLAN is not tied to a mobility network (that is, its traffic is locally bridged), the Fast Ethernet interface must be configured as an 802.1q trunk and those specific VLANs must be supported on the attached switch interface. Traffic generated as part of a mobility network is sent over the native VLAN. To configure multiple encryption schemes, begin by defining a VLAN for each mobility group and a native VLAN as shown in Figure 12.

**Figure 12  Access Point—Defining VLANs**

The next step is to define any encryption used by each VLAN as shown in Figure 13.
Figure 13  Access Point—Defining Per VLAN Encryption

The last step is to define SSIDs with mobility network-IDs and any authentication settings and map them to VLANs as shown in Figure 14.

Figure 14  Access Point—Defining SSIDs With Mobility Network IDs

Review the configuration on the CLI as shown in the following script:

```
interface Dot11Radio0
no ip address
no ip route-cache

! --Of the mobility networks that will use encryption, configure encryption types:
  encryption vlan 11 mode ciphers ckip
  encryption vlan 12 key 2 size 128bit 7 320E1C172908192BDC1668324160 transmit-key
  encryption vlan 12 mode wep mandatory

! --Define each SSID and specify a VLAN, authentication, and mobility network ID.
```

! --SSID "seagle-leap" uses LEAP authentication with a CKIP cipher
ssid seagle-leap
  vlan 11
    authentication open eap eap_methods
    authentication network-eap eap_methods
    mobility network-id 101
!
! --SSID "seagle-open" uses open authentication and no encryption
ssid seagle-open
  vlan 10
    authentication open
    mobility network-id 100
!
! --SSID "seagle-staticWEP" uses Open Authentication and a 128 bit static WEP key
ssid seagle-staticWEP
  vlan 12
    authentication open
    mobility network-id 102

  speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
  rts threshold 2312
  station-role root
!
! --Radio subinterfaces are automatically created for each defined VLAN.
! --The native VLAN (a "locally bridged" VLAN) carries
! --administrative traffic and mGRE tunneled traffic to the upstream switch
interface Dot11Radio0.1
  encapsulation dot1Q 1 native
  no ip route-cache
  bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
    bridge-group 1 spanning-disabled
!
interface Dot11Radio0.10
  encapsulation dot1Q 10
  no ip route-cache
  bridge-group 10
    bridge-group 10 subscriber-loop-control
    bridge-group 10 block-unknown-source
    no bridge-group 10 source-learning
    no bridge-group 10 unicast-flooding
    bridge-group 10 spanning-disabled
!
interface Dot11Radio0.11
  encapsulation dot1Q 11
  no ip route-cache
  bridge-group 11
    bridge-group 11 subscriber-loop-control
    bridge-group 11 block-unknown-source
    no bridge-group 11 source-learning
    no bridge-group 11 unicast-flooding
    bridge-group 11 spanning-disabled
!
interface Dot11Radio0.12
  encapsulation dot1Q 12
  no ip route-cache
  bridge-group 12
    bridge-group 12 subscriber-loop-control
    bridge-group 12 block-unknown-source
    no bridge-group 12 source-learning
no bridge-group 12 unicast-flooding
bridge-group 12 spanning-disabled

interface Dot11Radio1
no ip address
no ip route-cache
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled

interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto

! --Subinterfaces are also created on the wired side for every VLAN
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled

interface FastEthernet0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
no bridge-group 10 source-learning
bridge-group 10 spanning-disabled

interface FastEthernet0.11
encapsulation dot1Q 11
no ip route-cache
bridge-group 11
no bridge-group 11 source-learning
bridge-group 11 spanning-disabled

interface FastEthernet0.12
encapsulation dot1Q 12
no ip route-cache
bridge-group 12
no bridge-group 12 source-learning
bridge-group 12 spanning-disabled

interface BVI1
ip address 10.91.104.108 255.255.255.192
no ip route-cache

ip default-gateway 10.91.104.65
ip http server
ip radius source-interface BVI1
bridge 1 route ip

wlccp ap username cisco password 7 045802150C2E
wlccp ap wds ip address 10.0.100.2
wlccp ap mobility
!
line con 0
line vty 0 4
   login local
line vty 5 15
   login
!
end

In the above configuration, the Fast Ethernet switch port that the access point attaches to does not need to be configured as an 802.1q trunk because only one locally bridged VLAN is present. However it may be necessary to configure the Fast Ethernet interface on the attached switch as an 802.1q trunk if more than one VLAN is configured and not tied to a mobility network.

**Additional Considerations**

**IP Addressing for Mobile Clients**

Devices that associate to an SSID mapped to a mobility network have either a statically defined IP address or will use DHCP (Dynamic Host Control Protocol) to obtain an address.

One of the optional commands within a tunnel configuration is the `mobility trust` command. This command allows client devices to pass traffic using a statically assigned IP address.

For security reasons, it is recommended that mobile devices be assigned an IP address by a DHCP server. The DHCP server can reside on the Supervisor 720 or elsewhere on the network. For a DHCP server on the Supervisor module, use the following example to configure the server.

```
ip dhcp excluded-address 172.16.1.0 172.16.1.20
ip dhcp excluded-address 172.16.2.0 172.16.2.20
!
ip dhcp pool mobilenet1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.1
!
ip dhcp pool mobilenet2
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.1
!
```

Also, a global command, `ip dhcp snooping` is required for `dhcp snooping`. This command is used to reveal IP address assignments of mobile nodes and must be set globally as well as on a tunnel basis. The global form of the command is:

```
Sup720...(config)# ip dhcp snooping
```

For DHCP servers residing on a router other than the Supervisor 720, be sure to use an IP Helper Address on the tunnel configuration. The helper address takes a broadcast request for an address from the client and unicasts it to the DHCP server.
Fast Secure Roaming

The fast secure roaming feature enables wireless clients to quickly roam between access points residing on the same subnet. Using CCKM (Cisco Centralized Key Management), the WDS caches security keys derived for a client’s session and provides them to a destination access point when a client roams. By caching this information rather than forcing the client to reauthenticate to a centralized server, the authentication time is lessened and the total time required to roam is reduced.

Fast secure roaming works at Layer 2. Fast secure roaming also works over Layer 3 mobility because the mGRE tunnel architecture creates a virtual subnet. All access points participating in a particular mobility network support clients on a single subnet. The WLSM provides the WDS for that subnet and caches the security credentials for its mobile clients.

To enable Fast Secure Roaming on an SSID using the GUI, configure the access point as shown in Figure 15.

Figure 15  Access Point—Configuring Fast Secure Roaming on an SSID
To enable fast secure roaming on an SSID from the CLI, enter the following commands:

```plaintext
ssid seagle-leap
   vlan 11
   authentication open eap eap_methods
   authentication network-eap eap_methods
      authentication key-management cckm
   mobility network-id 101
```

**IP Multicast**

The administrative messages in IP Multicast (for example, *joins* and *leaves*) are sent over the locally bridged network. The locally bridge network is either the native VLAN or a VLAN created specifically for this purpose.

Actual multicast traffic in the upstream direction (from wireless network to wired), is sent within the tunnel architecture along with unicast and broadcast traffic. In the downstream direction (from wired to wireless), IP multicast traffic is locally bridged. In order to accommodate this traffic, a separate VLAN must be configured for each network with multicast capabilities.

**Fragmentation**

Tunneling technology is susceptible to fragmentation because of the overhead (an additional 24 bytes per packet) added to a user’s data packets as they enter the tunnel. Depending on the size of the packet sent by the client and the IP Maximum Transmission Unit (MTU) of the access point and the Catalyst 6500, traffic may get dropped.

A common issue that may cause traffic to be dropped occurs when a client’s MTU is greater than the MTU size of the tunnel and the client’s traffic is marked as DF (don’t fragment). The receiving device (Catalyst 6500 or access point) must drop the traffic since it cannot add the tunnel header without exceeding the MTU and is not allowed to break the packet into smaller pieces with separate headers.

For troubleshooting purposes, do not set `no ip unreachables` on the tunnel interface, thereby preventing ICMP unreachable messages from being sent to the sender (which would indicate a possible MTU issue).

To test the effect of the MTU on traffic delivery, send 1518 Byte data packets from a wireless client to a wired device across a mobility network. Then send the same size packets in the opposite direction. Investigate the MTU if any of the traffic is dropped.

As a general guideline, the IP MTU should be set to a number less than or equal to the smallest setting on all devices in both the upstream (towards the Catalyst 6500) and downstream (towards the access point) directions minus the tunnel header’s extra 24 bytes. Based on a 1500 byte minimum packet size, the recommended IP MTU would be less than or equal to 1476 Bytes. Setting this parameter on the tunnel interface on the Supervisor 720, dynamically passes it to the access point during tunnel setup. The default IP MTU setting is 1476 Bytes. There is no need to modify it unless it has been previously reconfigured. For more information about tunneling and fragmentation refer to Cisco.com:

Configure the WLSE for WDS

The CiscoWorks Wireless LAN Solution Engine (WLSE) provides many features for managing the wireless LAN, including the following:

- Making configuration changes
- Providing reports
- Collecting radio monitoring and management information
- Performing device discovery

For some features, such as RF management, the WLSE collects information from access points and clients throughout the network. In order to receive RF management information, the WLSE must be registered with the WDS in the same way that an access point must be registered with the WDS in order to provide it.

In order for the WLSE to communicate with WDS, the following configurations must be present:

- The WLSE must have LEAP credentials configured (referred to as WLCCP credentials)
- The WDS must be a managed device on the WLSE
- The WDS must be informed of the location of the WLSE

The first of these configurations involves browsing to the WLSE and selecting WLCCP Credentials under the Discover section of the Devices tab as shown in Figure 16.

![Figure 16 WLSE—Defining LEAP Credentials](image)

Enter the LEAP username and password pair that the WLSE will pass to the WDS. Be sure that this username/password pair is properly configured as a user in the RADIUS database on the CiscoSecure ACS server.

The next step is to manage the WDS from the WLSE. Before a device can be managed by WLSE, both devices must be configured for SNMP. The WLSE is configured as shown in Figure 17.
Note

These same community strings must also be configured on the WLSM/WDS.

The CLI configuration is as follows:

```bash
WLSM# config t
WLSM(config)# snmp-server view iso iso included
WLSM(config)# snmp-server community public view iso RO
WLSM(config)# snmp-server community private view iso RW
```

Once configured, the WDS appears in the device discovery on the WLSE (Figure 18) and is either automatically managed (if configured to do so) or provides the administrator the option of managing it. With the state of the device as managed, the WLSE attempts to register with the WDS (after the WDS is configured with the IP address of the WLSE server).
On the WDS, specify the IP address of the Wireless Network Manager (WNM). The WNM in the current Cisco SWAN environment is the WLSE.

The following script shows how to specify the WNM IP address using the CLI,

```
wlccp wnm ip address 10.91.104.79
```

In the Reports section of the Device Manager tab on the WLSE, the WNM should reflect being successfully authenticated with WDS, as shown in Figure 19.

**Figure 19  WLSE—Successful WDS Authentication**
Configurations

The following sections contain CLI configuration scripts.

WLSM Configuration

WLSM...#sh run
Building configuration...

Current configuration : 1243 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname WLSM...
!
logging queue-limit 100
enable password rfrus
!
username admin password 0 cisco
spd headroom 512
aaa new-model
!

aaa authentication login infrastructure-authentication group radius
aaa authentication login client-authentication group radius
aaa session-id common
ip subnet-zero
ip tftp source-interface Ethernet0/0.100
!

wlan vlan 100
ipaddr 10.0.100.2 255.255.255.0
gateway 10.0.100.1
admin
!
!
!
!
!
!
!
!
!
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.100.1
ip http server
no ip http secure-server
!
no cdp run
snmp-server view iso iso included
snmp-server community public view iso RO
snmp-server community private view iso RW
snmp-server enable traps tty
radius-server host 10.91.104.76 auth-port 1645 acct-port 1645
radius-server key cisco
radius-server authorization permit missing Service-Type
!
wlccp authentication-server infrastructure infrastructure-authentication
wlccp authentication-server client any client-authentication
wlccp wnm ip address 10.91.104.79
!
line con 0
line 1 3
no exec
transport input all
flowcontrol software
line vty 0 4
password cisco
!
end
WLSM...#

Supervisor 720 Configuration

(Line Card Configurations Deleted)

Sup720...#sh run
Building configuration...

Current configuration : 6352 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service counters max age 10
!
hostname Sup720...
!
boot system sup-bootflash:s72033-jsvdbg-mz.ROCKIES_SPL_040628
logging snmp-authtail
enable password 7 04490D141A32
!
no aaa new-model
wlan module 1 allowed-vlan 100
ip subnet-zero
!
ip dhcp excluded-address 172.16.1.0 172.16.1.20
ip dhcp excluded-address 172.16.2.0 172.16.2.20
!
ip dhcp pool mobilenet1
  network 172.16.1.0 255.255.255.0
  default-router 172.16.1.1
!
ip dhcp pool mobilenet2
  network 172.16.2.0 255.255.255.0
  default-router 172.16.2.1
!
ip dhcp snooping
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
mode rpr-plus
main-cpu
  auto-sync running-config
  auto-sync standard
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
interface Loopback100
  description tunnel_source
  ip address 10.80.0.1 255.255.255.255
!
interface Loopback101
  description tunnel_source
  ip address 10.80.0.2 255.255.255.255
!
interface Tunnel100
  description To_wireless_clients
  ip address 172.16.1.1 255.255.255.0
  no ip redirects
  ip mtu 1476
  ip dhcp snooping packets
tunnel source Loopback100
tunnel mode gre multipoint
mobility network-id 100
mobility trust
mobility broadcast
!
interface Tunnel101
  description To_wireless_clients
  ip address 172.16.2.1 255.255.255.0
  no ip redirects
  ip dhcp snooping packets
tunnel source Loopback101
tunnel mode gre multipoint
mobility network-id 101
mobility trust
mobility broadcast
!

interface Vlan1
  ip address 10.91.104.100 255.255.255.192
!
interface Vlan100
  ip address 10.0.100.1 255.255.255.0
!
router eigrp 100
  redistribute connected
  network 10.91.104.0 0.0.0.255
  network 172.16.0.0
  auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.91.104.65
no ip http server
!
Access Point Configuration – Single Encryption Scheme

```
seagle_ap1#sh run
Building configuration...

Current configuration : 1890 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname seagle_ap1
!
logging queue-limit 100
enable secret 5 $1$EGx1$d.0irqIr99x5pV4v9yByG0
!
username Cisco password 7 070C285F4D06
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers ckip
!
ssid seagle-leap
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management cckm
  mobility network-id 100
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
```
interface Dot11Radio1
  no ip address
  no ip route-cache

  ssid tsunami
    authentication open
    guest-mode

  speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
  rts threshold 2312
  station-role root
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
  bridge-group 1 spanning-disabled

interface FastEthernet0
  no ip address
  no ip route-cache
duplex auto
  speed auto
  bridge-group 1
  no bridge-group 1 source-learning
  bridge-group 1 spanning-disabled

interface BVI1
  ip address 10.91.104.108 255.255.255.192
  no ip route-cache
  ip default-gateway 10.91.104.65
  ip http server
     /122-15.JA/1100
  ip radius source-interface BVI1
  bridge 1 route ip

wlccp ap username cisco password 7 030752180500
wlccp ap wds ip address 10.0.100.2

line con 0
line vty 0 4
  login local
line vty 5 15
  login

end

Access Point Configuration – Multiple Encryption Scheme

seagle_ap1#sh run
Building configuration...

Current configuration : 3588 bytes

version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname seagle_ap1
!
logging queue-limit 100
enable secret 5 $1$EGx1$d.0irqIr99x5pV4v9yRyG0
!
username Cisco password 7 070C285F4D06
ip subnet-zero
!
!
bridge irb
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  
  encryption vlan 11 mode ciphers ckip
  
  encryption vlan 12 key 2 size 128bit 7 320E1C172908192BDC1668324160 transmit-key

  encryption vlan 12 mode wep mandatory
  
  ssid seagle-leap
  vlan 11
  
  authentication open eap eap_methods
  
  authentication network-eap eap_methods
  
  authentication key-management cckm
  
  mobility network-id 101
  
  ssid seagle-open
  vlan 10
  
  authentication open
  
  mobility network-id 100
  
  ssid seagle-staticWEP
  vlan 12
  
  authentication open
  
  mobility network-id 102
  
  speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
  
  rts threshold 2312
  
  station-role root
  
  interface Dot11Radio0.1
  encapsulation dot1Q 1 native
  no ip route-cache
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
  bridge-group 1 spanning-disabled
  
  interface Dot11Radio0.10
  encapsulation dot1Q 10
  no ip route-cache
  bridge-group 10
  bridge-group 10 subscriber-loop-control
  bridge-group 10 block-unknown-source
  no bridge-group 10 source-learning
no bridge-group 10 unicast-flooding
bridge-group 10 spanning-disabled
!
interface Dot11Radio0.11
encapsulation dot1Q 11
no ip route-cache
bridge-group 11
bridge-group 11 subscriber-loop-control
bridge-group 11 block-unknown-source
no bridge-group 11 source-learning
no bridge-group 11 unicast-flooding
bridge-group 11 spanning-disabled
!
interface Dot11Radio0.12
encapsulation dot1Q 12
no ip route-cache
bridge-group 12
bridge-group 12 subscriber-loop-control
bridge-group 12 block-unknown-source
no bridge-group 12 source-learning
no bridge-group 12 unicast-flooding
bridge-group 12 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.10
encapsulation dot1Q 10
no ip route-cache
bridge-group 10
no bridge-group 10 source-learning
bridge-group 10 spanning-disabled
!
interface FastEthernet0.11
encapsulation dot1Q 11
no ip route-cache
bridge-group 11
no bridge-group 11 source-learning
bridge-group 11 spanning-disabled
!
interface FastEthernet0.12
encapsulation dot1Q 12
no ip route-cache
bridge-group 12
no bridge-group 12 source-learning
bridge-group 12 spanning-disabled
!
interface BVI1
  ip address 10.91.104.108 255.255.255.192
  no ip route-cache
  !
  ip default-gateway 10.91.104.65
  ip http server
  ip radius source-interface BVI1
  bridge 1 route ip
  !
  !
wlc cp ap username cisco password 7 110A1016141D
  wlc cp ap wds ip address 10.0.100.2
  !
  line con 0
  line vty 0 4
    login local
  line vty 5 15
    login
  !
end
Figure 20 shows a configuration map of the configurations discussed in this document.