Chris Bryant, CCIE #12933 **http://www.thebryantadvantage.com/**

Back To Index

WLAN Configuration And Monitoring Tools

Overview

Autonomous WLANs

The Wireless LAN Solution Engine

Lightweight WLANs And The WLAN Controller

WCS Versions

The Location Appliance And RF Fingerprinting

Configuring A Wireless LAN Controller

Using The WLC GUI

Using The WCS And Adding A WLC

Detecting Rogue APs With The WCS

"Hot Spots And Gotchas"

Autonomous WLANs And The WLSE

We have two choices when it comes to WLAN models:

- Autonomous
- Lightweight

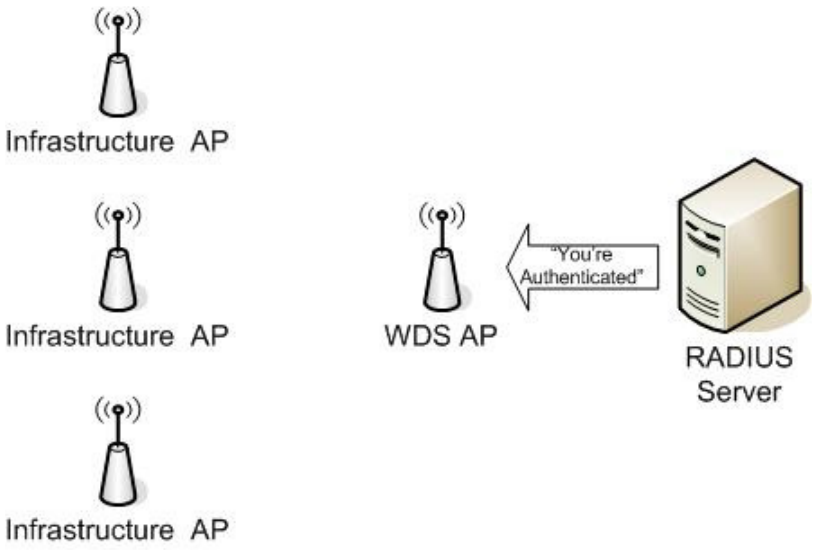
Those terms aren't exactly self-explanatory, so let's examine each option.

With an autonomous WLAN implementation, the APs are configured individually - there is no WLAN Controller. We do have the option of using ***CiscoWorks Wireless Lan Solution Engine (WLSE)*** to configure the autonomous APs. We'll discuss the WLSE and its cousin, *WLSE*

Express, later in this section.

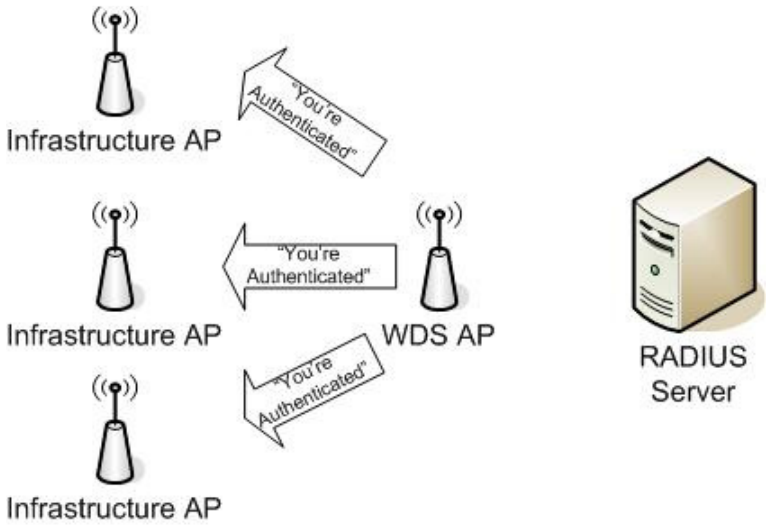
Wireless Domain Services (WDS) plays an important role in an autonomous WLAN implementation as well. A common method of using WDS is to configure one of the autonomous APs as the WDS device; all other APs ("infrastructure APs") will use the *WLAN Context Control Protocol* to communicate with the WDS AP.

While the WDS AP will need to authenticate to an external RADIUS server...



... the infrastructure APs will authenticate to the WDS AP if that particular AP has authenticated before.

If this is the first time the infrastructure AP has authenticated, the request will be passed through to the RADIUS server. The WDS AP will then cache the authentication information for future reference.



CiscoWorks Wireless Lan Solution Engine (WLSE)

The CiscoWorks WLSE acts as the manager of the autonomous APs. If there's a need to change the config on the APs, we've got two choices:

- Perform them on each individual AP
- Perform the change on the WLSE

Not much of a choice there, especially if we're working with hundreds of APs! CiscoWorks WLSE has quite a few features to help make our WLANs run smoothly:

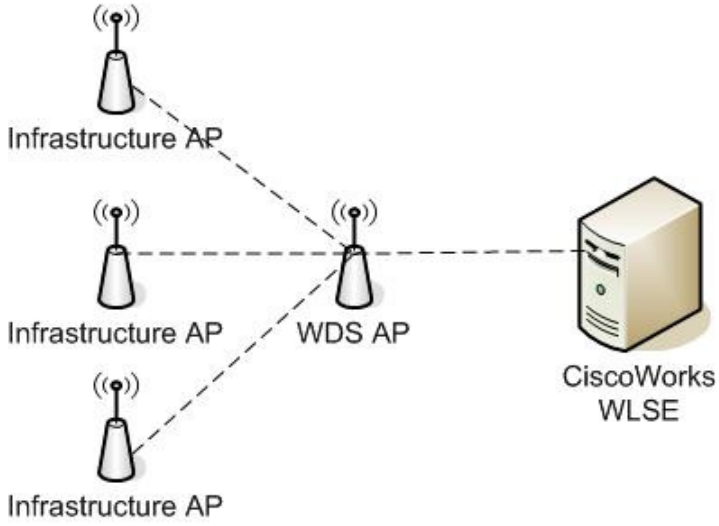
- Proactive monitoring of thresholds and alerting the admin to potential issues before they become critical, which assists with capacity planning and monitoring network performance as new clients are added
- Reporting and tracking features to help with problem diagnosis, troubleshooting, and resolution
- Centralized AP configs allow us to change multiple AP configs simultaneously
- Execute multiple firmware upgrades simultaneously
- Creation of templates that can be used to quickly configure new APs, which makes configuration of multiple APs much more efficient than configuring them individually
- Very effective at detecting rogue APs and can then either take action to shut that rogue AP down or notify the admin of the rogue AP's presence
- When an AP is lost, WLSE will tell that AP's neighbors to increase their cell coverage ("*self-healing network*")

There are two versions of WLSE. The full version (generally referred to as

simply "WLSE") can manage a maximum of 2500 devices. *WLSE Express* is for smaller networks that have 100 or fewer devices to manage.

One important setup difference between the two - the Express version has an *integrated* AAA server; the "regular" version does not, so you will need an *external* AAA server for use with the full version.

Once the deployment is complete, the infrastructure APs are communicating with the WDS AP, and the WDS AP is in turn sending any necessary information to CiscoWorks WLSE.



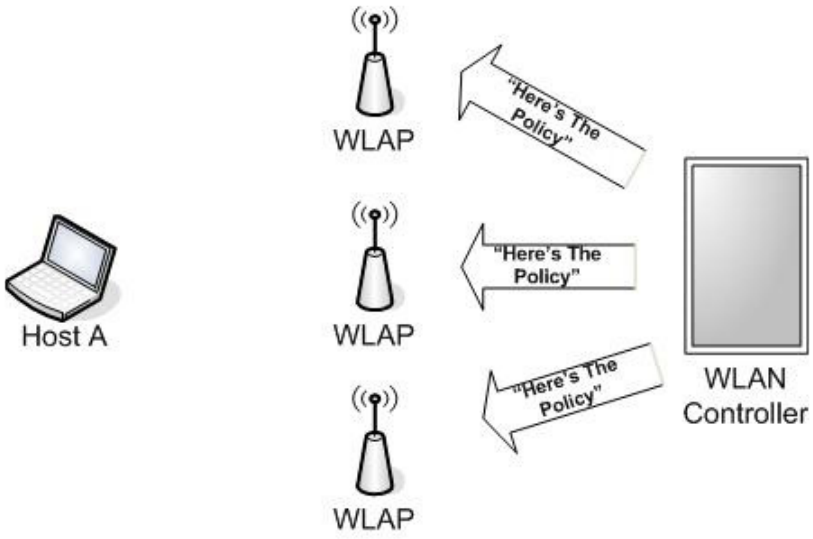
The limit on the number of APs is determined by the device in use as the WDS:

- If the WDS device is an AP, the limit is 60.
- If it's an Integrated Services Router, the limit is 100.
- If it's a switch running WLSM (Wireless LAN Services Module), the limit is 600.

Remember that all limits are theoretical and your mileage may vary!

Lightweight WLANs And WLCs

The lightweight WLAN implementation is the one we saw in the Wireless sections - a combination of *Lightweight Wireless Access Points* (LWAPs) and a central *WLAN Controller* (WLC).

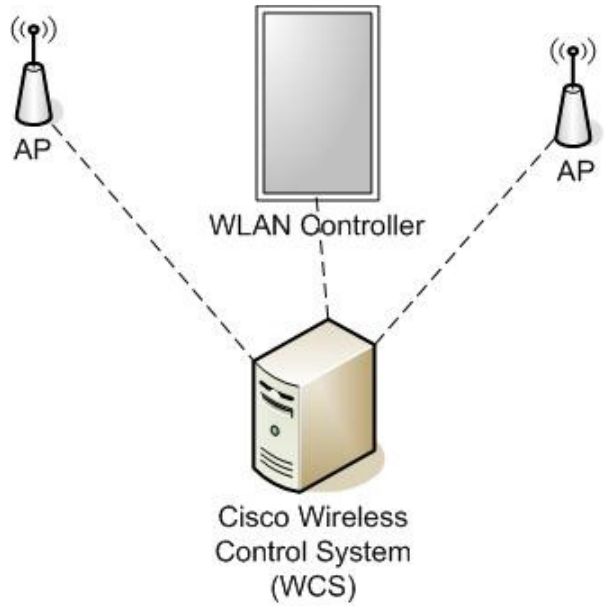


While the lightweight WLAN implementation is generally considered more scalable, note that each implementation type has a centralized point of control.

Lightweight WLAN implementations use the following for WLAN management:

- *Wireless Control System* (WCS)
- *Location Appliance*

The WCS serves as the manager for a lightweight deployment. AP configuration, accounting, security, performance tracking, intrusion detection features - they're all available on the WCS. The WCS can communicate with both APs and WLAN Controllers.



The WCS will actually generate and display - gasp! - *graphics* to illustrate the WLAN Controllers and APs. We'll take a long look at the WCS and its options later in this section.

We'll go over some specifics in the next section of this chapter, but I do want to mention now that the WCS can run on Windows or Linux - many admins prefer Linux for this task - and communications between the WCS and WLC are handled by SNMP. Watch your ACLs and do not inadvertently block SNMP.

Planning For WCS Deployment

Let's take a look at the dreaded "minimum server requirements" for a WCS deployment - and from personal experience, I can tell you the key word there is "*minimum*"!

- Windows 2000: SP 4 or higher
- Windows 2003: SP 3 or higher
- Red Hat Enterprise Linux: ES v.3
- HD should be 20 GB *minimum*

Whether you choose Windows or Linux, you can run WCS as an application or as a service.

WCS can be configured via Secure HTTP, and it supports SNMP v1, v2, and v3. WCS can also be configured via the CLI, and that's actually required when first configuring the Wireless Location Appliance (more about that later).

If you try to configure WCS via a non-secure HTTP connection, you'll receive a message that your connection is being changed to HTTPS.

Other requirements are dependent on how many APs you're going to have:

- 500 or less: 2.4 GHz Pentium w/ 1 GB RAM (again, minimum)
- 500 + APs: You'll need dual processors, each should be at least 2.4 GHz, and at least 2 GB RAM

A real-world word of warning: Don't go cheap on RAM.

Finally, the client must be running IE 6.0 SP1 or later.

WCS Versions

Now that we've got the hardware taken care of, we have to decide on which version of WCS to run. We have three choices, listed in order of capabilities from lowest to highest:

- Base
- Location
- Location w/ 2700 Series Location Appliance ("plus 2700")

I'm not downtalking Base by saying it has the least capabilities, but Location w/ the Location Appliance is *fantastic*!

All three versions will offer the basics - AP autodiscovery, central point of configuration, and tracking and monitoring capabilities among them - but a major difference between Base and Location is their capability to zero in on a rogue AP.

With WCS Base, we get the *approximate* location of a rogue AP. When a genuine AP detects a rogue, WCS Base is notified and then calculates the approximate location of the rogue AP from the signal strength of the genuine AP that initially reported the rogue.

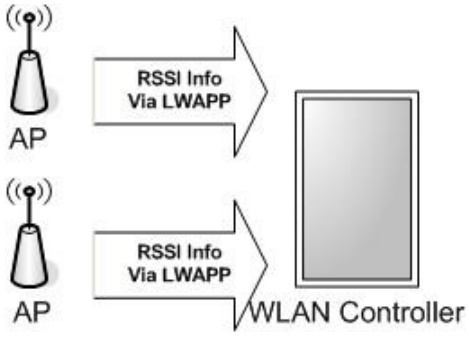
According to Cisco documentation, WCS Location can zero in on the location of a rogue AP to *within 10 meters*!

If WCS Location is so great, why use Location +2700? The main appeal of that appliance is the capability to track up to 1500 devices simultaneously, where Location allows tracking of only one device.

The Location Appliance And RF Fingerprinting

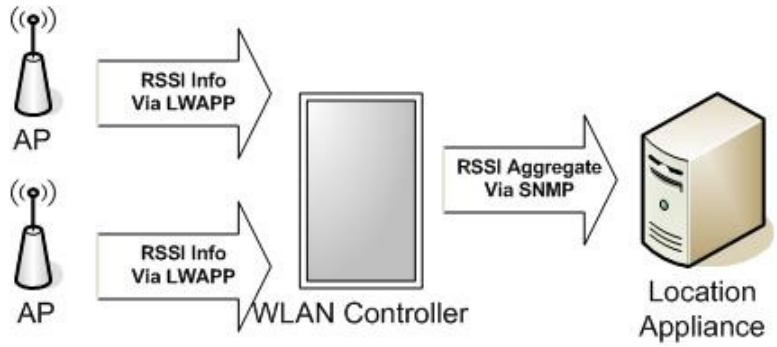
Your fingerprints can prove who you are; they can also prove who you are not. In a similar vein, a device's *RF Fingerprint* can prove that it is a legitimate access point - or prove that it is not!

All of the devices in our WLAN have a role in RF Fingerprinting. The APs themselves will collect *Received Signal Strength Indicator information (RSSI),* and will send that information to the WLAN Controller (WLC) via LWAPP.



In turn, the WLAN Controller will send the RSSI information it receives from the APs to the Location Appliance. That information is sent in a summarized ("aggregated") form.

Note that Simple Network Management Protocol is used to do this; again, make sure not to block SNMP communications between the two devices.



What else can be tracked in the Location Appliance?

- Laptop and palm clients
- RFID Asset Tags (Radio Frequency Identifier)
- VoIP clients

Some other Location Appliance notes

- The default username and pw are both "admin".
- The default port used by the server is 8001.
- The initial configuration must be performed at the good ol' CLI, not in a browser.

Configuring A Wireless LAN Controller

I doubt this shows up on your ONT exam, but since the WLC I'm using in the following lab had no previous configuration, I thought I'd show you the initial prompts from the WLC. Interesting that when I entered "n" for *no*, the WLC would not accept it.

```
Enter Administrative User Name (24 characters max): cisco

Enter Administrative Password (24 characters max): *****

Management Interface IP Address: 10.6.1.50
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.6.1.100
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 4
Management Interface DHCP Server IP Address: 10.6.1.50

AP Manager Interface IP Address: 10.6.1.51
```

```
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.6.1.50): 10.6.1.50

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: Group1

Network Name (SSID): WLC4
Allow Static IP Addresses [YES][no]: n
Invalid response

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code (enter 'help' for a list of countries) [US]: SI

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration...

Resetting system with new configuration...

    Cisco Bootloader (Version 3.2.195.10)



                   .o88b. d888888b .d8888.  .o88b.  .d88b.
                  d8P  Y8   `88'   88'  YP d8P  Y8 .8P  Y8.
                  8P         88    `8bo.   8P      88    88
                  8b         88      `Y8b. 8b      88    88
                  Y8b  d8   .88.   db   8D Y8b  d8 `8b  d8'
                   `Y88P' Y888888P `8888Y'  `Y88P'  `Y88P'


                                Model AIR-WLC2006-K9   S/N: FTX11028080

Booting Primary Image...
Press <ESC> now for additional boot options...
Detecting hardware . . . .
```

At that point, you'll see about 50 lines referring to starting given services such as DHCP Server, QoS services, and LWAPP.

After that, you'll be prompted for a username and password. Since this is the first login after a new username and pw were configured, we have an interesting option:

```
Enter User Name (or 'Recover-Config' this one-time only to reset
configuration to factory defaults)
```

```
User: cisco
Password:*****
(Cisco Controller) >
```

Since I didn't want to reset the WLC, I entered the username / password I had just configured, and that puts us at the Cisco Controller prompt.

Interestingly enough, I then stepped away for a few minutes and saw this when I came back:

```
*** IDLE TIMEOUT ***
```

Logging back in was no problem...

```
User:
User:cisco
Password:*****
(Cisco Controller) >
```

IOS Help works in the same fashion on a WLC as it does on a router:

```
(Cisco Controller) >?

clear          Clear selected configuration elements.
config         Configure switch options and settings.
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout         Exit this session. Any unsaved changes are lost.
ping           Send ICMP echo packets to a specified IP address.
reset          Reset options.
save           Save switch configurations.
show           Display switch options and settings.
transfer       Transfer a file to or from the switch.
```

show sysinfo is a great place to start troubleshooting a WLC, or just to become familiar with its settings.

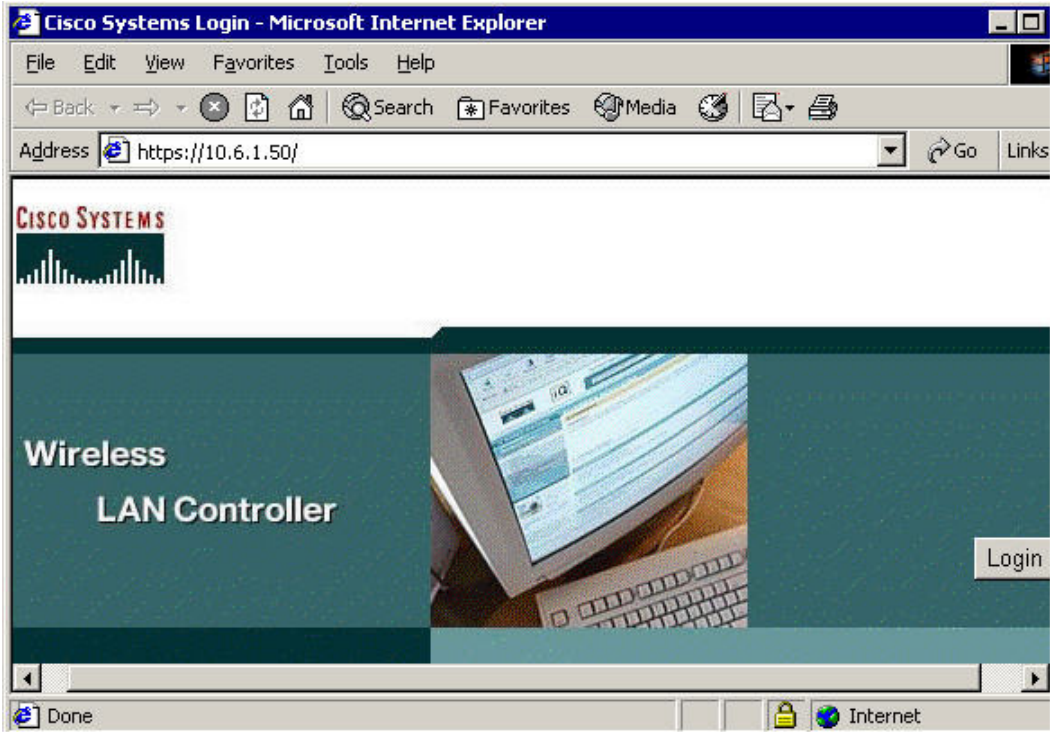
```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 3.2.195.10
RTOS Version..................................... 3.2.195.10
Bootloader Version............................... 3.2.195.10
Build Type....................................... DATA + WPS
Compact Flash Size............................... 256 MB

System Name...................................... Cisco_47:ec:00
System Location.................................
System Contact..................................
System                          ObjectID.....................................
1.3.6.1.4.1.14179.1.1.4.2
IP Address....................................... 10.6.1.50
System Up Time................................... 0 days 0 hrs 23 mins 8
secs

Configured Country............................... SI  - Slovenia
```

```
State of 802.11b Network..................... Enabled
State of 802.11a Network..................... Disabled
Number of WLANs.............................. 1
3rd Party Access Point Support............... Disabled
--More-- or (q)uit
Number of Active Clients..................... 0
```

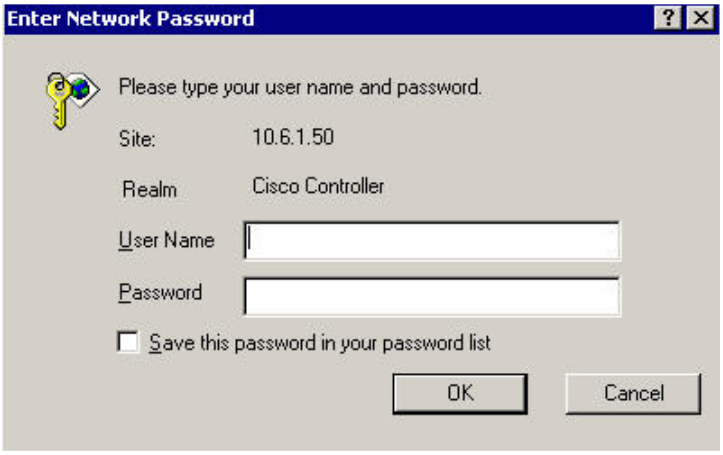
Once we've concluded the initial configuration at the CLI, we can use a web browser to access the GUI.

Using The WLC GUI

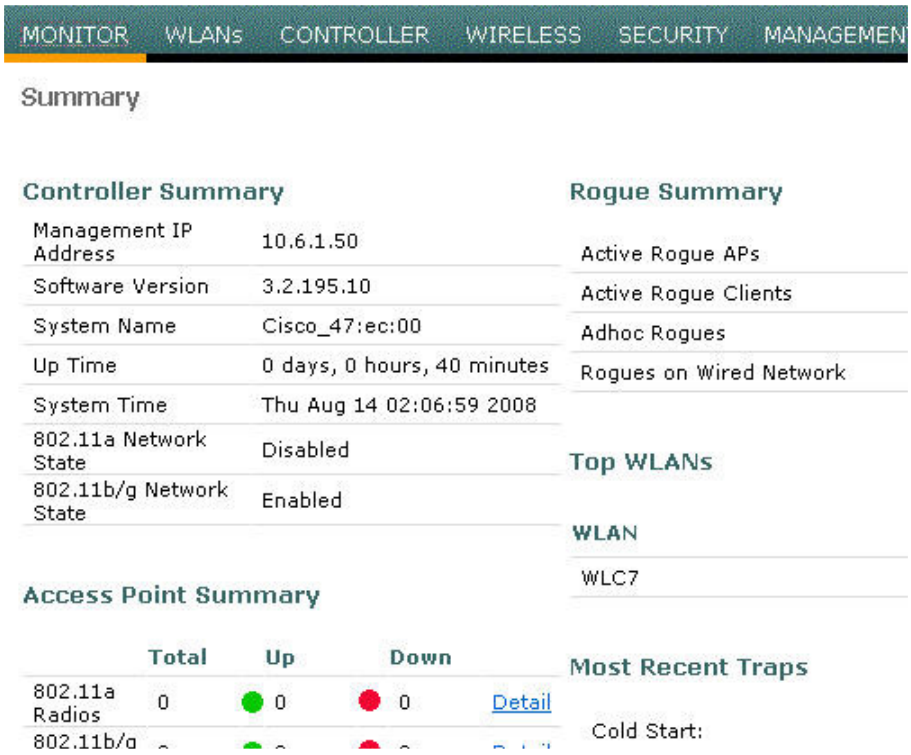
We'll launch the WLC GUI and browse to the WLC's management address of 10.6.1.50 - note that this is a secure connection via HTTPS.



Click the login button and we're off!



Well, almost! Now we need to enter a valid username and password for the WLC, and then we're off! We'll then be taken to the *Summary* screen.



We can't quite see the entire AP Summary, so I then scrolled down and here's what we have... or don't have!

Access Point Summary

	Total	Up	Down
802.11a Radios	0	0	0
802.11b/g Radios	0	0	0
All APs	0	0	0

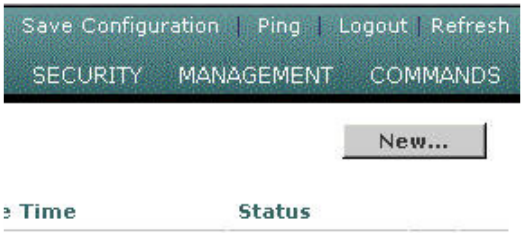
We'll now configure the WLC to act as an Internal DHCP Server. To do so, choose Controller at the top of the screen, which will then present you with this menu on the left-hand side of the screen:

Obviously, we'll choose *Internal DHCP Server*.

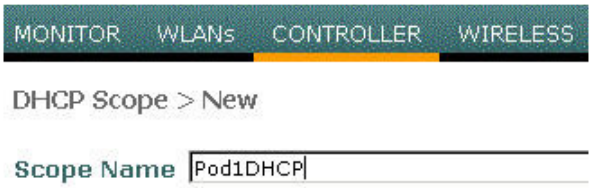
DHCP Scopes

Scope Name	Address Pool	Lease Time	Status

We have no scopes, so let's fix that. At the very far right-hand corner of this screen, you'll see a *New...* button. (You'll have to scroll over to see it - it's practically hidden.)

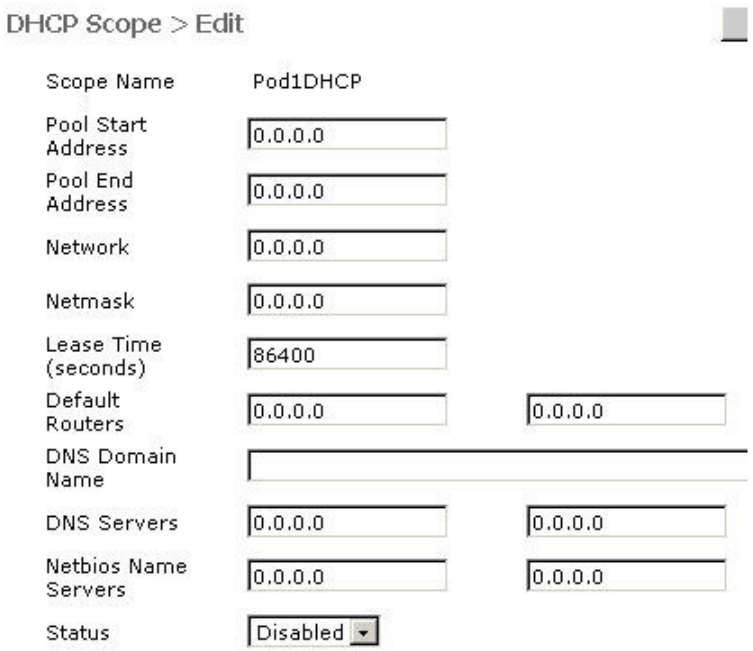


Once you click that, you'll be prompted to name this particular pool.



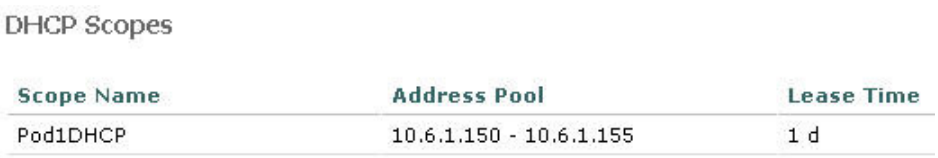
Click the also-practically-hidden *Apply* button, and we're back at the Scope screen.

Click Edit, and we're presented with this screen:

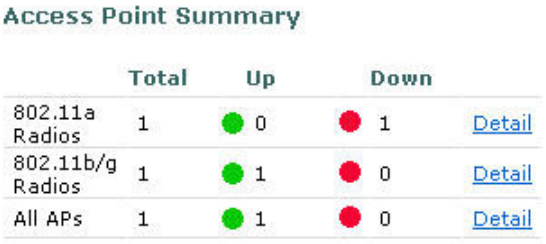


Fill in the desired information and click *Apply.* Don't forget to change the status from Disabled to Enabled!

The DHCP Scope now shows the addresses I entered:



And now when we go back to the Summary screen, we see wireless APs that have gotten their IP address and configuration info from this WLC.



The WLC Summary page refreshes every 30 seconds, so you don't have to keep hitting F5 when you expect information there to change - say, like these APs appearing!

Notice that the .11a radio is detected, but showing as down? That's

because way back when we configured the WLC....

```
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
```

... we didn't enable .11a!

Just for fun, I clicked *Details* next to the b/g access point, and this information comes up:

802.11b/g Radios

AP Name	Base Radio MAC	Admin Status	Operational Status
Pod7AP	00:0b:85:6d:65:c0	Enable	UP

Way to the right of all of this information is a *Configure* link.

Admin Status	Operational Status	Channel	Power Level	Antenna		
Enable	UP	6	5	Internal	Configure	Detail

When you go to the Configure screen, you'll be presented with two rows of config choices. Here's the first one...

802.11b/g Cisco APs > Configure

General

AP Name	Pod7AP
Admin Status	Enable
Operational Status	UP
Site Config ID	0

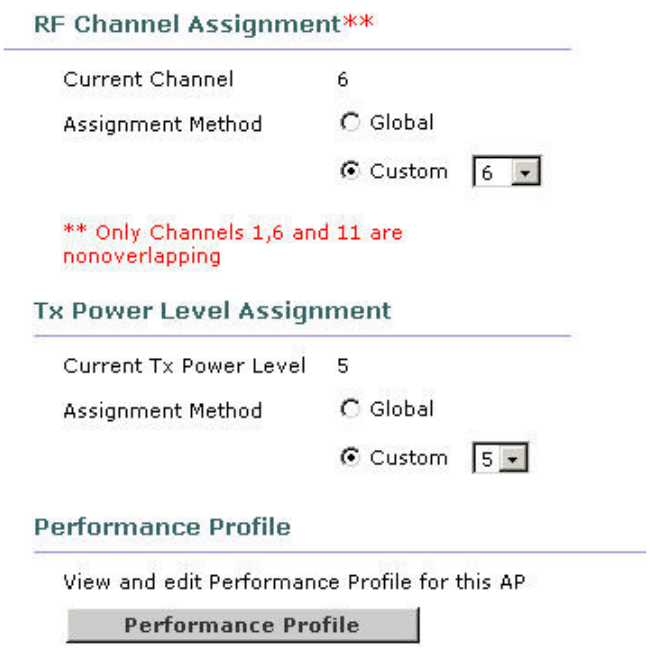
Antenna

Antenna Type	Internal
Diversity	Enabled

WLAN Override

WLAN Override	Disable

.. and here's the second.



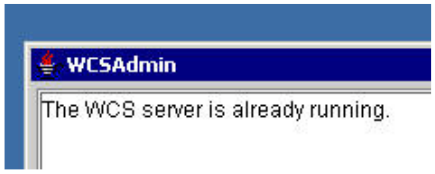
The reasons we'd change any of these are beyond the scope of the ONT exam, but I did want to show you where these values can be changed. The WLC is almost as easy to get around in as SDM is - you just have to scroll a lot more with the WLC!

Configuring WCS And Adding A WLC

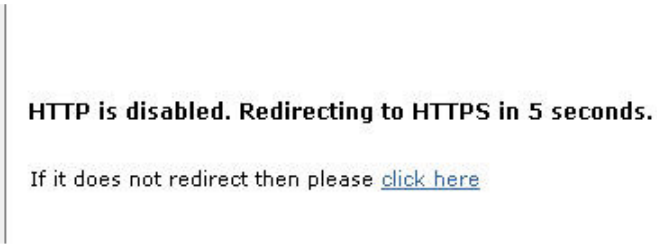
After installing WCS on a server, you'll see these icons on the desktop:

After clicking *StartWCS,* we receive the following message:

If WCS is already running, you'll get a message that the WCS Service is already running.



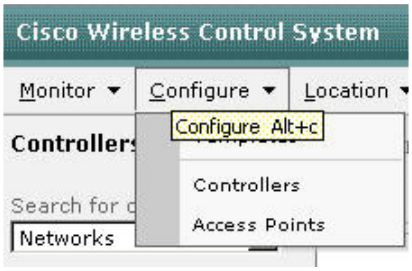
A secure HTTP connection is required. Here, I attempted a non-secure connection, and I received this message:



I then launched a browser and a secure connection to 127.0.0.1, which brings us to the Wireless Control System login window.

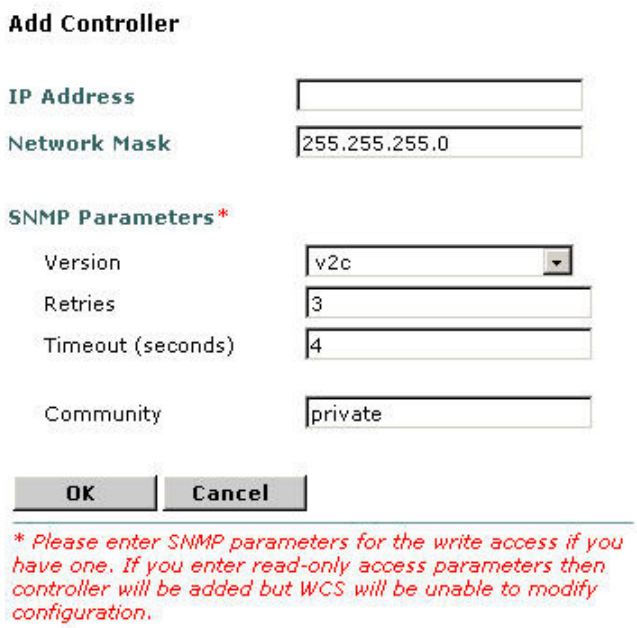
After logging in, we're brought to the main window.

Since we use the WCS to manage WLCs, we better know how to add a WLC with this tool! To do so, just click *Configure* and then *Controllers* in the drop-down box. (The word hidden by "Configure Alt-c" is "Templates". This drop-down box really doesn't like dropping down and *staying* there!)



On the next screen, select *Add Controller* in the drop-down box and click *Go.*

Here's the next screen:



After entering the IP address and mask for the management interface on the WLC, we see the following message - hopefully for just a short time!

When WCS discovers the WLC, you'll see the IP address of the controller appear just above "Add Controller" and a message that the controller has been successfully added to WCS.

If you attempt to find a WLC with an incorrect IP address, you'll see the following message instead.

That status message doesn't exactly narrow things down, does it?

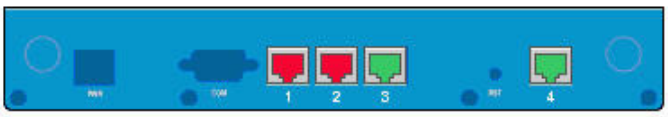
To see all WLCs, use this drop-down menu path: *Monitor > Devices > Controllers.* The IP address of the WLCs will be hyperlinked:

Controllers > Search Results

IP Address	Controller Name	Type	Location	Mobility Group Name	Reachability Status
10.6.1.50	Pod1WLC	2000		Group1	Reachable

Click on the address for a detailed summary of the WLC.

Controllers > 10.6.1.50 > Summary



General

IP Address	10.6.1.50
Name	Pod1WLC
Type	2000
UP Time	0 days 1 hrs 8 mins 2 secs
System Time	Sat Aug 16 15:56:00 2008
Location	
Total Client Count	1
Current LWAPP Transport Mode	Layer3

Total APs 1

Alarms

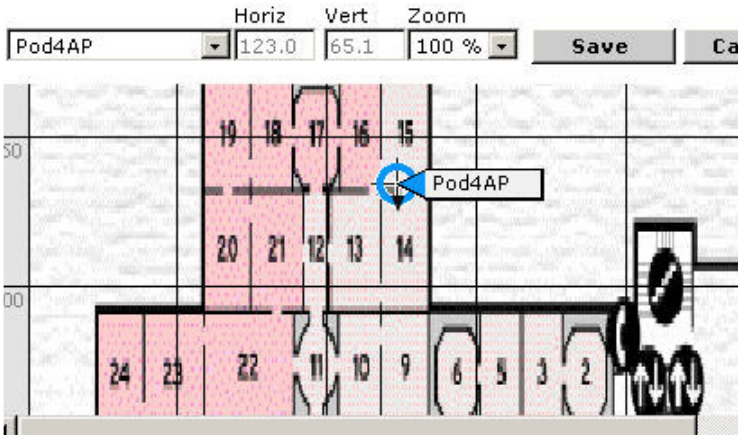
Events

Utilization

Utilization (%)
40

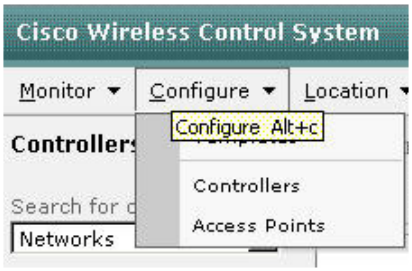
Using the Map function of WCS is beyond the scope of the ONT exam, but I do want to give you an idea of what it looks like:

Position access points on Floor Area 'Me'



You can create floor plans, create maps showing Access Points, gauge who would and would not be able to hit the APs, and so much more. If you do get the chance to work with the Maps feature in WCS in a lab or production environment, I will say it takes a little getting used to, but it can be a very powerful tool for planning, implementing, and monitoring your wireless network!

Before we head for the review, let's take another look at this screen:

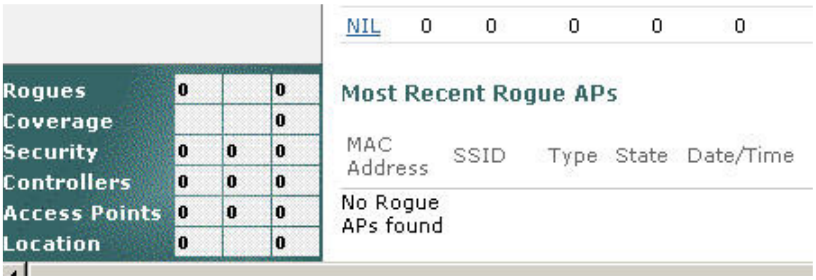


We looked at Monitor and Configure, but not Location. That choice allows you to add and configure Location Appliances.

Detecting Rogue Access Points

The WCS can also detect rogue access points and minimize their effect on your network. When one of the WLCs detects a rogue AP, that WLC will send a notification to the WLC that a new rogue AP has been found.

On the Monitor screen of our WCS, we see no rogue APs have been detected - if there had been, some of the white cells here would turn red to indicate a problem:



The next action is dependent on the level of AP containment you've configured in WCS. Available options are 1 AP, 2 AP, 3 AP, and 4 AP. If you choose 1 AP, one AP near the rogue AP will send *deauthenticate and disassociate* messages to the clients that have formed an association with that rogue AP. If you choose 2 AP, two APs will send these messages, and so forth.

The WLC will then continue to monitor the rogue AP until that rogue is either eliminated or acknowledged as a non-threatening rogue.

"Hot Spots And Gotchas"

This is obviously a large chapter, so don't just read the summary! :) Having said that, let's review the high points:

I won't put them all here again, but be sure to review the many uses of the WLSE listed at the very beginning of this section. The WLSE and Wireless Domain Services (WDS) are used to manage an autonomous WLAN.

The WLSE comes in both "regular" and Express forms. WLSE Express has an integrated AAA server, but the regular version of WLSE requires an external AAA server.

For lightweight WLANs, a combination of the Cisco WCS and WCS Location Appliance are used to configure and manage the network.

The WCS

As we saw in the lab, the WCS can do it all - you can plan your network using the Maps option, and then configure and manage your WLCs and APs (the Map option helps with that as well).

As we also saw in the lab, when we used the browser to open WCS, HTTPS was used.

The WCS uses SNMP to communicate with the WLCs, so be sure not to accidentally block that communication with an ACL.

Both the WCS and the Appliance must be configured initially at the CLI.

You can run WCS on either a Windows or Linux box.

WCS helps to detect and shut down rogue APs, but there's one major difference between WCS Base and Location - Base gives you a general idea of the location of the AP, where Location can nail the rogue AP's location down to just a few yards.

There were icons on the desktop to both start and stop WCS, as well as check WCS status and uninstall it as well.

Typical menu paths in WCS:

Adding A WLC: Configure > Controllers, then click Add Controller and GO. On the next screen, enter the IP address and mask of the management interface on the WLC and click OK. You'll then see a message indicating either that the WLC was found or not found.

Viewing All WLCs: *Monitor > Devices > Controllers.* For additional information on each WLC, click the hyperlinked IP address.