



Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





SBA

BORDERLESS
NETWORKS

DEPLOYMENT
GUIDE

Wireless LAN CleanAir Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide	1	Troubleshooting with CleanAir	12
Cisco SBA Borderless Networks.....	1	Accessing Remote CleanAir for Spectrum Expert.....	12
Route to Success.....	1		
About This Guide.....	1	Appendix A: Product List	15
Business Overview	2	Appendix B: Changes	17
Technology Overview	3		
Cisco CleanAir Technology.....	3		
Cisco Prime NCS.....	3		
Deployment Details	4		
Installing Cisco NCS.....	4		
Adding Wireless LAN Controllers to Cisco NCS.....	5		
Adding Buildings and Floor Plans.....	6		
Configuring the Cisco Wireless Solution for CleanAir.....	9		

What's In This SBA Guide

Cisco SBA Borderless Networks

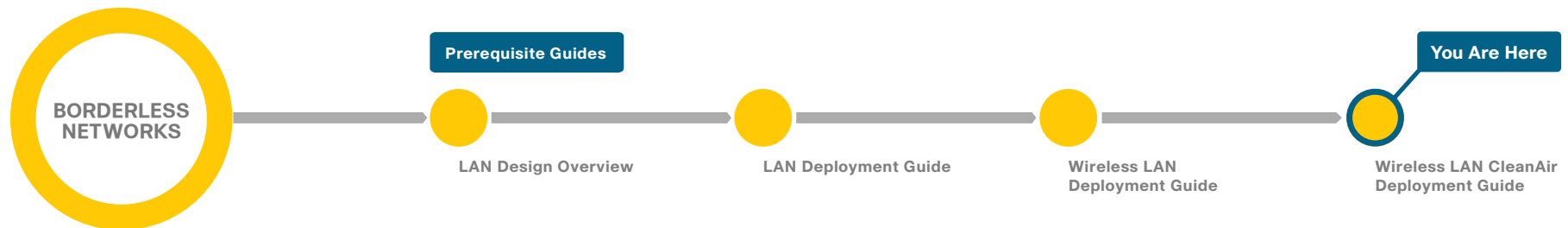
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

Business Overview

The challenges of running a wired data network are beyond the expectations of most other jobs. The challenges go beyond simply adding a machine and handing it over to the desktop IT department or to the end user to leverage as they desire. Of the numerous challenges that arise with any application, the network is always the easiest entity to blame for failure. Now add a *wireless* data network to the picture, and you triple the challenges and skill set required to maintain and troubleshoot the network. Wireless networking brings a new set of unknowns that an administrator of a wired network never had to address.

Wi-Fi is no longer just a convenient technology used for casual web surfing or simple connectivity from conference rooms. With 802.11n, wireless performance is now on par with wired networks, and businesses and organizations, such as hospitals, rely on the wireless network for mission-critical and patient-critical applications. Without running expensive site surveys with a spectrum analyzer every hour and minute of every day, the network administrator cannot tell what is happening in the user space. With limited IT resources and a lack of RF expertise, an organization requires tools to alert for potentially negative issues before a user creates a call ticket in the network call center.

Notes

Technology Overview

Cisco CleanAir Technology

Cisco CleanAir technology is the integration of Cisco Spectrum Expert Wi-Fi analysis tools with Cisco access points. Before CleanAir technology was released, operators had to walk around with an instrument to detect signals of interest and physically locate the device that generated them. CleanAir helps to automate these tasks within the system management function by adding additional intelligence over Cisco Spectrum Expert, thereby augmenting the overall experience in proactively reclaiming control over the radio spectrum.

The components of a basic Cisco CleanAir solution are the Cisco Wireless LAN Controller and Cisco Aironet 2600 or 3600 Series access points. To take advantage of the entire set of CleanAir features, Cisco Network Control System (NCS) can display in real-time the data retrieved from CleanAir. Adding Cisco Mobility Services Engine (MSE) further enhances the available features and provides the history and location of specific interference devices.

Cisco NCS with Cisco CleanAir technology allows network administrators to visually see how well their network is performing, remotely troubleshoot client connectivity, manage wireless network resources, analyze interference devices from anywhere in the world, and more. The real power of NCS with CleanAir combined with Cisco access points is the ability to visually represent the radio environment to the network administrator, so the administrator can better manage and troubleshoot issues before they bring the network to its knees.

Cisco Prime NCS

Cisco Prime NCS, part of Prime Infrastructure, enables you to configure and monitor one or more Cisco wireless LAN controllers and associated access points, monitor and troubleshoot radio technology, and visually display Cisco CleanAir data to the network administrator. Cisco NCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level, and adds a graphical view of multiple controllers and managed access points.

Cisco Prime NCS offers both physical appliance and virtual appliance deployment options, providing full product functionality, scalability, ease of installation, and setup tailored to your deployment preference.

Notes

Deployment Details

For the deployment described in this guide, Cisco NCS is deployed as a virtual appliance. The largest virtual appliance supports up to 15,000 Cisco Aironet lightweight access points, 5000 standalone access points, and 1200 Cisco wireless LAN controllers. A low-end virtual appliance supports up to 3000 Cisco Aironet lightweight access points, 1000 standalone access points, and 240 Cisco wireless LAN controllers.

Process

Installing Cisco NCS

1. Deploy Cisco NCS OVA
2. Configure Cisco NCS basic settings
3. Log in to Cisco NCS and install license files

Procedure 1 Deploy Cisco NCS OVA

Step 1: Cisco Prime NCS is provided as an Open Virtual Appliance (OVA). The OVA is prepackaged with disk, memory, CPU, NICs, and other virtual machine related configuration parameters. This is an industry standard, and many virtual appliances are available in this format. A different OVA file is provided for each virtual appliance model.

Step 2: Deploy Open Virtualization Format (OVF) Template with VMWare vSphere client.

You must first install the Cisco Prime NCS OVA on the VMware ESX/ESXi server using vSphere before configuring the virtual appliance.

Step 3: After the virtual appliance has been deployed and configured, turn on the appliance. The first time you turn on the appliance you need to enter the default login credentials: **root/password**.

Procedure 2

Configure Cisco NCS basic settings

Step 1: At the setup prompt, enter **setup**. When you turn on the appliance for the first time, you see the setup prompt, as shown below.

```
*****
Please type 'setup' to configure the appliance
*****
localhost.localdomain login: setup
```

Step 2: Enter the following server configuration details:

- Hostname (Example: NCS)
- IP Address (Example: 10.4.48.19)
- IP Netmask (Example: 255.255.255.0)
- Default Gateway (Example: 10.4.48.1)
- DNS Domain Name (Example: cisco.local)
- Primary Name Server (Example: 10.4.48.10)
- Add/Edit another name server? Y/N (Example: N)
- Primary NTP Server (Example: 10.4.48.17)
- System Time Zone (Example: America/Los_Angeles)

Step 3: Enter the username for the account used to access the Cisco NCS system running on the virtual machine. The default username is admin, but you can change this to another username.

Step 4: Enter and confirm a system admin password.

Step 5: Enter **No** when prompted with Will this server be used as a Secondary for HA?

Step 6: Enter and confirm the password for the root account to use to log in to Cisco Prime NCS using the browser. The password must be at least eight characters and must include both lowercase and uppercase letters and at least one number. It cannot include the username or default Cisco passwords.

Step 7: Enter and confirm the FTP user password.

Step 8: Enter **Y**. This applies the settings.

Procedure 3 Log in to Cisco NCS and install license files

Before starting, make sure that you have already acquired the license from the Cisco License Center and put it in a location that is accessible by the network from Cisco NCS. To add a new NCS license file, follow the steps below.

Step 1: Log in to the Cisco Prime NCS administration page using the credentials defined in the previous procedure. (Example: <https://ncs.cisco.local/>)

Step 2: In the Administrator menu, choose **License Center > Files > NCS Files**, and then click **Add**.

Step 3: In the Add a License File dialog box, enter or browse to the applicable license file.

Step 4: Once displayed in the License File text box, click **Upload**.

Repeat these steps for each license you have received.

Process

Adding Wireless LAN Controllers to Cisco NCS

1. Add controllers to Cisco NCS

You must add each wireless LAN controller to Cisco NCS so that you can monitor and centrally manage the network.

Procedure 1 Add controllers to Cisco NCS

Step 1: Navigate to **Configure > Controllers**.

Step 2: In the Select a command drop-down list, choose **Add Controllers**, and then click **Go**.

Step 3: In the Add Controllers dialog box, enter the following configuration details, and then click **Add**.

- IP addresses—**10.4.46.64, 10.4.46.65, 10.4.46.68, 10.4.46.69**
- SNMP Community—**cisco123**
- Protocol—**SSH**
- Username—**NCS**
- Password



Tech Tip

You can enter every controller IP address individually, separated by a comma, or you can select a comma-delimited (CSV) spreadsheet with the IP addresses of all controllers. In this example, a comma-separated list is used because all of the controllers in the organization use the same SNMP and SSH parameters.

Controllers Edit View								
Configure > Controllers								
-- Select a command -- Go								
Entries 1 - 4 of 4								
⏪ ⏩ ⏴ ⏵ ⏶ ⏷ ⏸ ⏹								
<input type="checkbox"/> IP Address	Device Name	Device Type	Location	SW Version	Mobility Group Name	Reachability Status	Inventory Collection Status	Audit Status
<input type="checkbox"/> 10.4.46.64	WLC5508-1	5500		7.2.110.0	CAMPUS	Reachable	Managed and synchronized	Identical
<input type="checkbox"/> 10.4.46.65	WLC5508-2	5500		7.2.110.0	CAMPUS	Reachable	Managed and synchronized	Identical
<input type="checkbox"/> 10.4.46.68	WLC7500-1	7500		7.2.110.0	REMOTES	Reachable	Managed and synchronized	Identical
<input type="checkbox"/> 10.4.46.69	WLC7500-2	7500		7.2.110.0	REMOTES	Reachable	Managed and synchronized	Identical
Entries 1 - 4 of 4								
⏪ ⏩ ⏴ ⏵ ⏶ ⏷ ⏸ ⏹								



Tech Tip

If you are getting timeout or communications errors when trying to add a controller, you may be running into an issue where there is more information requested than can fit into a single frame. To correct this, navigate to **Administration > Settings > SNMP Settings**, and then reduce the values for **Maximum VarBinds per Get PDU** and **Maximum VarBinds per Put PDU**.

Process

Adding Buildings and Floor Plans

1. Add the first campus and building
2. Place access points

The real advantage of any management system is that it can present information in a way that helps you make intelligent decisions. Cisco NCS brings visibility to the radio spectrum, which allows the administrator to see the coverage that is being provided to users. By including the building and floor maps in Cisco NCS, visibility of this otherwise unknown or convoluted data that NCS derives from the wireless network is enabled. You need to have an image of your floor plan before you begin this procedure. The file can be in JPEG, PNG, or GIF format; it can also be in CAD DXF or DWG format.

Add Controllers
Configure > Controllers > Add Controllers

General Parameters

Add Format Type: Device Info
IP Addresses: 10.4.46.64, 10.4.46.65, 10 (comma-separated IP Addresses)
Wism Auto Add

SNMP Parameters

Version: v2c
Retries: 2
SNMP Timeout: 10 (secs)
Community: *****

Telnet/SSH Parameters

Protocol: SSH
Username: NCS
Password: *****
Confirm Password: *****
Telnet Timeout: 60 (secs)

Add Cancel

The system tests connectivity to each controller you have specified and provides you with a list of your controllers, their host names, and the connectivity status of each, as shown in the following figure.

Procedure 1 Add the first campus and building

Even though you may have only one building today, you may end up with another building; or perhaps each campus is a single building today, but could have more buildings in the future. The campus, building, floor approach makes it easy to understand as you dig for more information and peel away the layers to find what you are looking for.

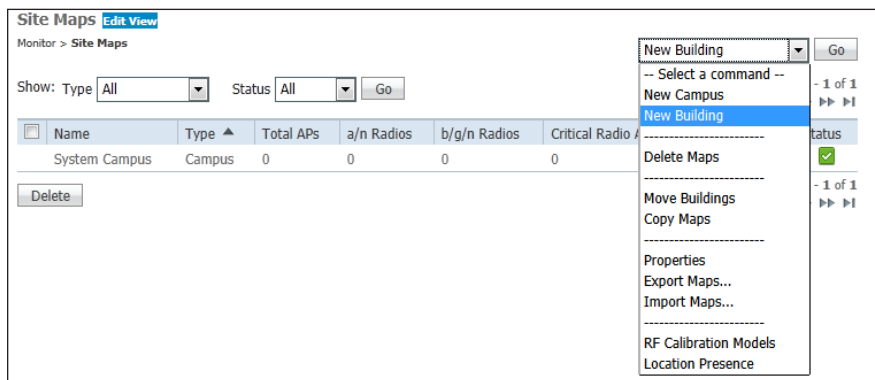


Tech Tip

You need to know the dimensions of the campus picture you are bringing into the system so that you can appropriately scale the drawing as each building and floor is added.

Step 1: In Cisco NCS, navigate to **Monitor > Site Maps**.

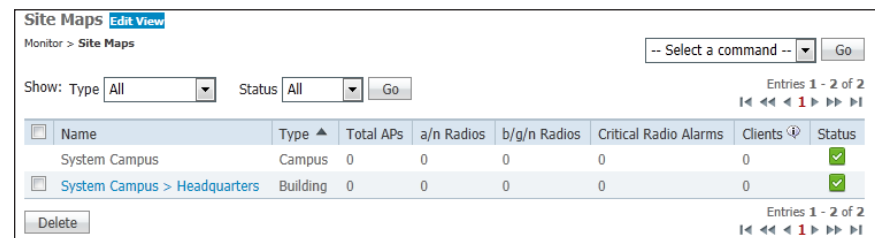
Step 2: In the Select a command drop-down list, choose **New Building**, and then click **Go**.



Step 3: Create the name of your building, specify the network administrator contact name, and enter the characteristics of the building:

- Building Name—**Headquarters**
- Contact—**SBA Admin**
- Number of floors—**1**
- Number of Basements—**0**
- Horizontal Span (feet)—**500**
- Vertical Span (feet)—**300**

Step 4: Select your newly created building.



Step 5: In the Select a command drop-down list, choose **New Floor Area**, and then click **Go**.

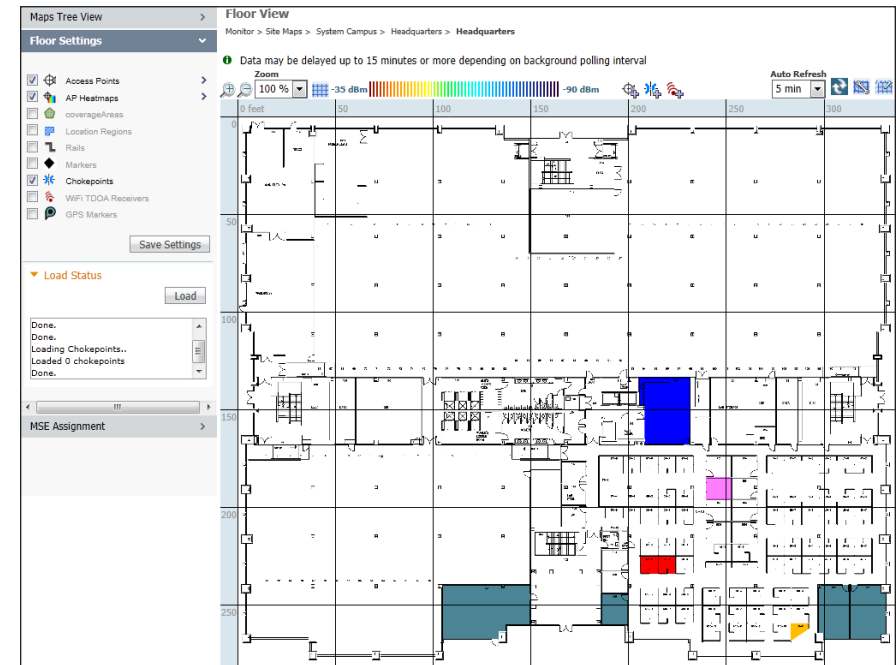
Step 6: Create a name for the floor area, specify the network administrator contact name, specify a floor number, and then create a description of the area.

- Floor Area Name—**SBA-Headquarters**
- Contact—**SBA Admin**
- Floor—**1**
- Floor Type (RF Model)—**Cubes And Walled Offices**
- Floor Height (feet)—**10.0**
- Image or CAD File—**C:\Headquarters.png**
- Convert CAD File to—**PNG**

Step 7: Select the floor plan image, and then click **Next**.

Step 8: Verify your new floor area details and image, and then click **OK**.

Step 2: Select your new floor area, SBA-Headquarters.



Step 3: In the Select a command drop-down list, choose **Add Access Points**, and then click **Go**.

Step 4: Select access points that are registered with the system but not yet placed for the headquarters building.

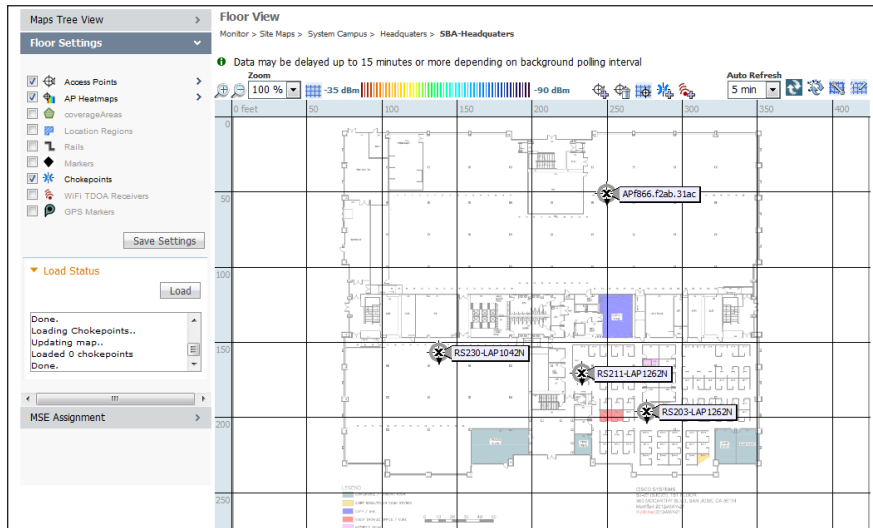
AP Name	MAC Address	AP Model	Controller
AP68ef.bda4.f0a6	08:1f:f3:e1:15:10	AIR-LAP1141N-A-K9	10.4.46.65
AP5475.d0ab.9210	1c:17:d3:cb:7e:a0	AIR-LAP1142N-A-K9	10.4.46.65
RS206-CAP3602I	64:d9:89:47:12:e0	AIR-CAP3602I-A-K9	10.4.46.68
RS213-CAP3602I	64:d9:89:47:17:90	AIR-CAP3602I-A-K9	10.4.46.68
RS207-CAP3602I	64:d9:89:47:60:10	AIR-CAP3602I-A-K9	10.4.46.68
RS210-LAP1262N	d0:57:4c:08:9f:10	AIR-LAP1262N-A-K9	10.4.46.68
RS223-LAP1142N	dc:7b:94:a4:3c:10	AIR-LAP1142N-A-K9	10.4.46.68
RS221-LAP1042N	0c:85:25:df:de:60	AIR-LAP1042N-A-K9	10.4.46.68
RS231-LAP1042N	0c:85:25:df:e1:f0	AIR-LAP1042N-A-K9	10.4.46.68
RS202-LAP1042N	0c:85:25:f2:af:30	AIR-LAP1042N-A-K9	10.4.46.68
AP0d00.f445.4abb	d0:57:4c:09:c0:60	AIR-LAP1262N-A-K9	10.4.46.69
RS204-LAP1262N	d0:57:4c:09:7c:a0	AIR-LAP1262N-A-K9	10.4.46.68
AP0d00.f445.4803	d0:57:4c:09:87:60	AIR-LAP1262N-A-K9	10.4.46.65
RS201-CAP3602I	64:d9:89:47:14:20	AIR-CAP3602I-A-K9	10.4.46.68
RS220-LAP1142N	dc:7b:94:a4:3f:e0	AIR-LAP1142N-A-K9	10.4.46.68
AP0d00.f445.4793	d0:57:4c:09:83:40	AIR-LAP1262N-A-K9	10.4.46.64

Procedure 2 Place access points

The final piece of the puzzle is to place the access points at the proper locations on your individual floor plans. If you take the time to place your access points where they are actually located, the wireless LAN controllers that work in conjunction with Cisco NCS give an accurate view of your network and the devices located in it.

Step 1: In Cisco NCS, navigate to **Monitor > Site Maps**.

Step 5: Carefully place each access point as close to its real position in the building as possible, and then click **Save**.



Wait while the system calculates the heat maps from the placement and floor plan area.

Process

Configuring the Cisco Wireless Solution for CleanAir

1. Create a Cisco CleanAir template
2. Enable EDRRM

A Cisco wireless LAN controller with connected Cisco Aironet 2600 or 3600 Series access points is immediately Cisco CleanAir-capable. The wireless LAN controllers can give you immediate information about your environment. Where Cisco NCS can take a complete network view, the wireless LAN controller displays only data retrieved from the locally connected CleanAir access points.

Cisco NCS can handle all management in the network. You can perform management tasks at each controller, but it is not recommended. With the Cisco CleanAir access point operating from the wireless LAN controller, you can log in to NCS and configure your controller to support CleanAir.

EDRRM

Event-driven radio resource management (EDRRM) is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A Cisco CleanAir access point always monitors Air Quality (AQ), and reports on AQ in 15-second intervals. AQ is a better metric than normal Wi-Fi chip noise measurements, because AQ only reports on classified interference devices. That makes AQ a reliable metric in that we know that what is reported is not caused by Wi-Fi energy (and hence is not a transient, normal spike).

The key benefit of EDRRM is very fast action time (30 seconds). If an interferer is operating on an active channel and is causing enough AQ degradation that it triggers EDRRM, clients cannot use that access point or channel. The only thing to do is get the access point off that channel. The EDRRM feature is not enabled by default. You must enable it in two steps: enable Cisco CleanAir, and then enable EDRRM.

Procedure 1

Create a Cisco CleanAir template

Step 1: In Cisco NCS, navigate to **Configure > Templates > Controller Template Launch Pad**.

Step 2: Navigate to **802.11a/n > CleanAir**.

Step 3: From the Select a command drop-down list, choose **Add Template**, and then click **Go**.

Step 4: Create a template with a meaningful name, provide the following information, and then click **Save**.

- Select **CleanAir Enable**.
- Select **Report Interferers Enable**.
- In the Interferers Selected for Reporting list, add **Continuous Transmitter**, **DECT-Like Phone**, **Jammer**, and **Video Camera**.
- Select **Interferers For Security Alarm Enable**.
- In the Interferers Selected for Security Alarms list, add **Continuous Transmitter**, **DECT-Like Phone**, **Jammer**, and **Video Camera**.

New Controller Template
Configure > Controller Template Launch Pad > 802.11a/n > CleanAir > New Controller Template

Template Name

CleanAir ☒ Enable

Reporting Configuration

Report Interferers ☒ Enable

Interferers Ignored for Reporting

- Canopy
- SuperAG
- TDD Transmitter
- WiFi Invalid Channel
- WiFi Inverted
- WiMAX Fixed
- WiMAX Mobile

Interferers Selected for Reporting

- Continuous Transmitter
- DECT-Like Phone
- Jammer
- Video Camera

Persistent Device Propagation ☐ Enable

Alarm Configuration

Air Quality Alarm ☐ Enable

Air Quality Unclassified category Alarm ☐ Enable

Interferers For Security Alarm ☒ Enable

Interferers Ignored for Security Alarms

- Canopy
- SuperAG
- TDD Transmitter
- WiFi Invalid Channel
- WiFi Inverted
- WiMAX Fixed
- WiMAX Mobile

Interferers Selected for Security Alarms

- Continuous Transmitter
- DECT-Like Phone
- Jammer
- Video Camera

Step 5: Click **Apply to Controllers**.

Step 6: Select the controllers to which you want to apply the template, and then click **OK**.

Step 7: Navigate to **802.11b/g/n > CleanAir**.

Step 8: From the Select a command drop-down list, choose **Add Template**, and then click **Go**.

Step 9: Create a template with a meaningful name, provide the following information, and then click **Save**.

- Select **CleanAir Enable**.
- Select **Report Interferers Enable**.
- In the Interferers Selected for Reporting list, add **Bluetooth Discovery**, **Bluetooth Link**, **Continuous Transmitter**, **DECT-Like Phone**, **Jammer**, **Microwave Oven**, **Video Camera**, and **Xbox**.
- Select **Interferers For Security Alarm Enable**.
- In the Interferers Selected for Security Alarms list, add **Bluetooth Discovery**, **Bluetooth Link**, **Continuous Transmitter**, **DECT-Like Phone**, **Jammer**, **Microwave Oven**, **Video Camera**, and **Xbox**.

Step 10: Click **Apply to Controllers**.

Step 11: Select the controllers to which you want to apply the template, and then click **OK**.

Procedure 2 Enable EDRRM

Step 1: Navigate to **Configure > Templates > Controller Template Launch Pad**.

Step 2: In the left pane, navigate to **802.11a/n > 802.11a/n-RRM > DCA**.

Step 3: In the Select a command drop-down list, choose **Add Template**, and then click **Go**.

Step 4: Create a template with a meaningful name, provide the following information, and then click **Save**.

- Select **Event Driven RRM Enable**.
- In the Sensitivity Threshold list, choose **Medium**.

New Controller Template
Configure > Controller Template Launch Pad > 802.11a/n > 802.11a/n-RRM > DCA > New Controller Template

General

Template Name: 802.11a/n-EDRRM

Dynamic Channel Assignment Algorithm

Assignment Mode: Automatic

Avoid Foreign AP Interference: ☐ Enable

Avoid Cisco AP load: ☐ Enable

Avoid non 802.11 Noise: ☐ Enable

Avoid Persistent Non-WiFi Interference: ☐ Enable

Signal Strength Contribution: ☒ Enable

Event Driven RRM

Event Driven RRM: ☒ Enable

Sensitivity Threshold: Medium

Save Cancel

Step 5: Click **Apply to Controllers**.

Step 6: Select the check boxes next to all controllers, and then click **OK**.

Step 7: Navigate to **Configure > Templates > Controller Template Launch Pad**.

Step 8: In the left pane, navigate to **802.11b/g/n > 802.11b/g/n-RRM > DCA**.

Step 9: In the Select a command drop-down list, choose **Add Template**, and then click **Go**.

Step 10: Create a template with a meaningful name, provide the following information, and then click **Save**.

- Select **Event Driven RRM Enable**.
- In the Sensitivity Threshold list, choose **Medium**.

Step 11: Click **Apply to Controllers**.

Step 12: Select the check boxes next to all controllers, and then click **OK**.

Troubleshooting with CleanAir

The real power of Cisco CleanAir is that a network administrator can stay on one continent while directly analyzing the Wi-Fi spectrum in another office on the other side of the planet. The Cisco Aironet 2600 and 3600 Series access points can be put in Spectrum Expert-Connect mode and used as a virtual remote interface for the knowledgeable engineer, no matter where this valuable human resource is located. By changing the role of your CleanAir access point and connecting the Cisco Spectrum Expert Wi-Fi 4.0 (or later) software, the Wi-Fi network administrator can view the environment directly. Your organization no longer needs to fly expensive personnel onsite to troubleshoot physical-layer issues that are challenging and, too often, intermittent.

Process

Accessing Remote CleanAir for Spectrum Expert

1. Configure Spectrum Expert Connect Mode

When the call for assistance arrives, it almost certainly will originate from a location that does not have the knowledgeable human resources to troubleshoot, identify, and fix the issue. Wi-Fi devices are designed to send and receive Wi-Fi signals, but they do not have the capability to identify non-Wi-Fi radio interferers, such as microwave ovens, Digital Enhanced Cordless Telecommunications (DECT) phones, analog wireless cameras, or even radio jammers. The specialized radios in the Cisco CleanAir radio environment can identify these devices and, with triangulation, can find where these devices are located.

When the call comes in, you need to identify as many facts about the issue as possible to make informed decisions. The information can include the location of the problem (for example, the street side of the building does not

have connectivity) and time of day (for example, the issue is pronounced at lunch time). With as much information from the end user as possible, you can now look at the radio environment because the system shows that clients are connecting and Cisco NCS indicates that AQ has dropped.

Procedure 1

Configure Spectrum Expert Connect Mode

The Cisco CleanAir-capable access point must be changed from either Monitor Mode or Local Mode of operation to Spectrum Expert Connect Mode (SE-Connect).

Step 1: Log in to the Wireless LAN Controller.

Step 2: Navigate to **WIRELESS**.

Step 3: Select the Cisco CleanAir access point that is closest to the suspected source of interference.

Step 4: In the AP Mode list, choose **SE-Connect**, and then click **Apply**.

Step 5: Wait for the access point to reboot and reconnect to the Wireless LAN Controller.

Wireless

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

All APs > Details for RS207-CAP36021

General Credentials Interfaces High Availability Inventory FlexConnect Advanced

General

AP Name: RS207-CAP36021

Location: RS207

AP MAC Address: 70:ca:9b:86:30:b0

Base Radio MAC: 64:d9:89:47:60:10

Admin Status: Enable

AP Mode: FlexConnect

AP Sub Mode: local

Operational Status: monitor

Port Number: Sniffer

Venue Group: Bridge

Venue Type: Unspecified

Venue Name:

Language:

Network Spectrum Interface Key: 21E8B83E88093C310D28258195493731

Versions

Primary Software Version: 7.2.110.0

Backup Software Version: 0.0.0.0

Predownload Status: None

Predownload Version: None

Predownload Next Retry Time: NA

Predownload Retry Count: NA

Boot Version: 12.4.23.0

IOS Version: 12.4(25e)JA1s

Mini IOS Version: 0.0.0.0

IP Config

IP Address: 10.5.20.21

Static IP: ☐

Time Statistics

UP Time: 0 d, 04 h 36 m 42 s

Controller Associated Time: 0 d, 02 h 46 m 01 s

Controller Association Latency: 0 d, 00 h 00 m 10 s

Hardware Reset

Perform a hardware reset on this AP

Reset AP Now

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Clear All Config

Clear Config Except Static IP

Foot Notes

1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.

Step 6: Copy the Network Spectrum Interface Key and the IP address.

Wireless

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless

All APs > Details for RS207-CAP36021

General Credentials Interfaces High Availability Inventory Advanced

General

AP Name: RS207-CAP36021

Location: RS207

AP MAC Address: 70:ca:9b:86:30:b0

Base Radio MAC: 64:d9:89:47:60:10

Admin Status: Enable

AP Mode: SE-Connect

AP Sub Mode: None

Operational Status: REG

Port Number: 1

Venue Group: Unspecified

Venue Type: Unspecified

Venue Name:

Language:

Network Spectrum Interface Key: 821B3CC03E76085FE0B4DF7BB386C733

Versions

Primary Software Version: 7.2.110.0

Backup Software Version: 0.0.0.0

Predownload Status: None

Predownload Version: None

Predownload Next Retry Time: NA

Predownload Retry Count: NA

Boot Version: 12.4.23.0

IOS Version: 12.4(25e)JA1s

Mini IOS Version: 0.0.0.0

IP Config

IP Address: 10.5.20.21

Static IP: ☐

Time Statistics

UP Time: 0 d, 00 h 06 m 33 s

Controller Associated Time: 0 d, 00 h 05 m 30 s

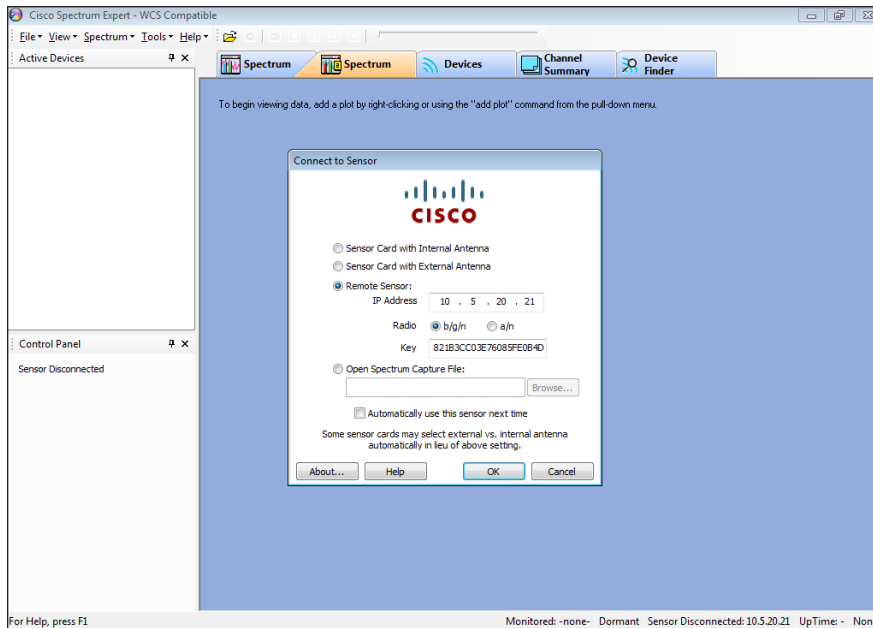
Controller Association Latency: 0 d, 00 h 01 m 02 s

Step 7: On a Supported Windows platform with Cisco Spectrum Expert Wi-Fi (4.0 or later) installed, launch Cisco Spectrum Expert.

Step 8: Select Remote Sensor.

Step 9: Enter the IP address and the Network Spectrum Interface Key of the CleanAir access point that you copied in Step 6.

Step 10: Select **b/g/n** for 2.4 GHz, or **a/n** for 5 GHz, and then click OK.



The connected Windows machine now connects to the remote Cisco CleanAir access point on UDP port 37540 (if you selected **b/g/n** in Step 10) or on UDP port 37550 (if you selected **a/n** in Step 10). If connection problems occur, verify that you can ping the CleanAir access point and that no network devices are blocking the necessary UDP port information.

Remote Spectrum Analysis

The remote sensor capability in Cisco Spectrum Expert gives you the ability to get real-time, physical-layer spectrum data without having to drive or fly onsite. The following figure illustrates this capability in a Wi-Fi-only environment and gives you an understanding of how it can show you what is really happening in your remote environment.



Tech Tip

Note that in the figure above, the Cisco Spectrum Expert does not detect a Wireless LAN card and that the remote sensor is at 10.5.20.21.

Appendix A: Product List

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	7.2.110.0
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco 7500 Series Wireless Controller for up to 1000 Cisco access points	AIR-CT7510-1K-K9	
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.2.110.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
On Site Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.2.110.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
CleanAir AP with 4x4 MIMO	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.2.110.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
CleanAir AP with 3x4 MIMO	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	7.2.110.0
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	

Network Management

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	1.2
	Prime Infrastructure 1.1 Software – 5K Device Base Lic	R-PI-1.1-5K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base Lic	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base Lic	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base Lic	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base Lic	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 50 Device Base Lic	R-PI-1.1-50-K9	

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We changed the management platform from Cisco WCS to Cisco NCS.
- We changed which access points are covered in this guide by removing the 3500 series access points and added the 2600 series access points.
- We made minor changes to improve the readability of this guide.

Notes

Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)