Lightweight Access Point FAQ

Document ID: 70278

You need a valid Cisco.com account in order to download Cisco Aironet drivers, firmware, and utilities from Downloads – Wireless (registered customers only **) . If you do not have a Cisco.com account, register for free at the Cisco.com Registration page.**

Contents

Introduction

This document provides information on the most frequently asked questions (FAQ) about Cisco Lightweight Access Points (LAPs).

Refer to Cisco Technical Tips Conventions for more information on document conventions.

LAP FAQ

Q. What is a Cisco Lightweight Access Point (LAP)?

A. The Cisco LAP is part of the Cisco Unified Wireless Network architecture. A LAP is an AP that is designed to be connected to a wireless LAN (WLAN) controller (WLC). The LAP provides dual band support for IEEE 802.11a, 802.11b, and 802.11g and simultaneous air monitoring for dynamic, real−time radio frequency (RF) management. In addition, Cisco LAPs handle time−sensitive functions, such as Layer 2 encryption, that enable Cisco WLANs to securely support voice, video, and data applications.

APs are lightweight, which means that they cannot act independently of a wireless LAN controller (WLC). The WLC manages the AP configurations and firmware. The APs are zero touch deployed, and individual configuration of APs is not necessary. The APs are also lightweight in the sense that they handle only real−time MAC functionality. The APs leave all the non−real−time MAC functionality to be processed by the WLC. This architecture is referred to as the split MAC architecture.

Q. Can I configure the LAP to operate independent of a wireless LAN controller (WLC)?

A. No, LAPs cannot function independent of WLCs. LAPs function in conjunction with a WLC only. The reason is that the WLC provides all the configuration parameters and firmware that the LAP needs in the registration process.

Q. What is Lightweight AP Protocol (LWAPP)?

A. LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run−time operations. LWAPP also defines the tunneling mechanism for data traffic.

A LAP discovers a controller with the use of LWAPP discovery mechanisms. The LAP sends an LWAPP join request to the controller. The controller sends the LAP an LWAPP join response, which allows the AP to join the controller. When the LAP joins to the controller, the LAP downloads the controller software if the revisions on the LAP and controller do not match. Subsequently, the LAP is completely under the control of the controller. LWAPP secures the control communication between the LAP and the controller by means of a secure key distribution. The secure key distribution requires already provisioned X.509 digital certificates on both the LAP and the controller. Factory−installed certificates are referenced with the term "MIC", which is an acronym for Manufacturing Installed Certificate. Cisco Aironet APs that shipped before July 18, 2005, do not have a MIC. So these APs create a self−signed certificate (SSC) when they are upgraded in order to operate in lightweight mode. Controllers are programmed to accept SSCs for the authentication of specific APs.

Q. What is CAPWAP?

A. In controller software release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points protocol (CAPWAP) in order to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is being implemented in controller software release 5.2 for these reasons:

- ♦ To provide an upgrade path from Cisco products that use LWAPP to next−generation Cisco products that use CAPWAP
- ♦ To manage RFID readers and similar devices
- ♦ To enable controllers to interoperate with third−party access points in the future

LWAPP−enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when you use CAPWAP are the same as when you use LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP−enabled software allows access points to join either a controller that runs CAPWAP or LWAPP. The only exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers that run CAPWAP. For example, an 1130 series access point can join a controller that runs either CAPWAP or LWAPP whereas an 1140 series access point can join only a controller that runs CAPWAP.

For more information, refer to the Access Point Communication Protocols section of the configuration guide.

Q. How do I distinguish between a regular (autonomous) AP and an LAP?

A. The easiest way to distinguish between a regular AP and a LAP is to look at the part number of the AP.

- ◆ LAP (Lightweight AP Protocol [LWAPP]) Part numbers *always* begin with **AIR−LAPXXXX**.
- ◆ Autonomous AP (Cisco IOS® Software) Part numbers *always* begin with **AIR−APXXXX**.

The Cisco Aironet 1000 Series LAPs are an exception to this criteria. The part numbers of the 1000 series LAPs are:

- ◆ AIR−AP1010−A−K9 for a 1010 LAP
- ◆ AIR−AP1020−A−K9 for a 1020 LAP
- ◆ AIR−AP1030−A−K9 for a 1030 LAP

Note: The part numbers can vary, which depends on the country and regulatory domain. The part numbers that this list provides are just examples.

Make sure that you order the appropriate AP for your wireless LAN (WLAN).

Q. Which AP models can run Lightweight AP Protocol (LWAPP)?

A. These Cisco Aironet AP platforms are able to run LWAPP:

- ◆ Aironet 1500 Series
- ◆ Cisco Aironet 1250 Series
- ◆ Aironet 1240 AG Series
- ◆ Aironet 1230 AG Series
- ◆ Aironet 1200 Series
- ◆ Aironet 1130 AG Series
- ◆ Aironet 1000 Series
- ◆ Aironet 1140 Series AP

Note: The 1140 Series AP is supported only with WLC that runs 5.2 release or later.
Note: You can order these Aironet APs with Cisco IOS Software to operate as autonomous APs or to operate with LWAPP. The part number determines if an AP is a Cisco IOS Software−based AP or an LWAPP−based AP. Here are examples:

- ◆ AIR−AP1242AG−A−K9 is a Cisco IOS Software−based AP.
- ◆ AIR−LAP1242AG−P−K9 is an LWAPP−based AP.

Note: The 1000 Series APs and the 1500 Series APs are exceptions to this criterion. All the 1000 Series APs and the 1500 Series APs support only LWAPP.

Q. How do I install and configure an LWAPP−enabled access point?

A. LWAPP−enabled APs are part of the Cisco Integrated Wireless Network Solution and require no manual configuration before they are mounted. The AP is configured by an LWAPP−capable Cisco Wireless LAN Controller (WLC). Refer to the Quick Start Guide LWAPP−Enabled Cisco Aironet Access Points for information on how to install and initially configure an LWAPP−enabled access point.

Q. How do I configure my LAP and my wireless LAN controller (WLC) together?

A. LAPs use Lightweight AP Protocol (LWAPP), and when they join a WLC, the WLC sends the LAPs all the configuration parameters and firmware. Refer to the Wireless LAN Controller and Lightweight Access Point Basic Configuration Example for a basic setup.

Q. Can I connect an autonomous AP to a wireless LAN controller (WLC) and expect the AP to work?

A. No, only LAPs work when they are connected to a WLC. Autonomous APs do not understand the Lightweight AP Protocol (LWAPP) or the CAPWAP protocol that the WLC uses. In order to connect an autonomous AP to a WLC, you must first convert the autonomous AP to lightweight mode.

Q. I have an autonomous Cisco IOS Software–based access point. Can I convert it to lightweight mode?

A. Yes, but not all the autonomous Cisco IOS Software–based AP models can be converted. These are the models that you can convert to Lightweight AP Protocol (LWAPP) mode:

- All Cisco Aironet 1130 AG APs
- All Aironet 1240 AG APs
- For all Cisco IOS Software–based Aironet 1200 Series modular AP (1200/1220 Cisco IOS Software upgrade, 1210, and 1230 AP) platforms, the ability to convert the AP depends on the radio.

    ◊ If the radio is IEEE 802.11g, MP21G and MP31G are supported.
    ◊ If the radio is IEEE 802.11a, RM21A and RM22A are supported.
    You can upgrade the 1200 Series APs with any combination of supported radios:

    ◊ G only
    ◊ A only
    ◊ Both G and A

Note: An autonomous AP must run Cisco IOS Software Release 12.3(7)JA or later before you can convert it to LWAPP.

Note: Only the Cisco 4400 and 2006 wireless LAN controllers (WLCs) support autonomous APs that have been converted to lightweight mode. Cisco WLCs must run a minimum software version of 3.1. The Cisco Wireless Control System (WCS) must run a minimum version of 3.1. The upgrade utility is supported on the Microsoft Windows 2000 and Windows XP platforms.

Refer to Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode for details on how to perform the conversion.

Q. What restrictions are imposed on a Cisco IOS Software–based access point after conversion to lightweight mode?

A. Keep these guidelines in mind when you use autonomous access points that have been converted to lightweight mode:

♦ APs that are converted to Lightweight AP Protocol (LWAPP) do not support Wireless Domain Services (WDS). LWAPP–converted APs communicate only with Cisco Wireless LAN (WLAN) Controllers (WLCs) and cannot communicate with WDS devices. However, the WLC provides functionality that is equivalent to the WDS when the AP associates to the WLC.

♦ Converted access points support 2006, 4400, and WiSM controllers only. When you convert an autonomous access point to lightweight mode, the access point can communicate with Cisco 2006 series controllers, 4400 series controllers, or the controllers on a Cisco WiSM only.

♦ In controller software release 4.2 or later, all Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. In previous releases, they supported only 8 BSSIDs per radio and a total of 8 wireless LANs per access point. When a converted access point associates to a controller, only wireless LANs with IDs 1 through 16 are pushed to the access point.

♦ APs that are converted to LWAPP must get an IP address and discover the WLC with use of DHCP, a Domain Name System (DNS), or an IP subnet broadcast.

♦ APs that are converted to LWAPP do not support Layer 2 LWAPP.

♦ APs that are converted to LWAPP provide a read–only console port.

♦ The upgrade conversion tool adds the self–signed certificate (SSC) key–hash to only one of the controllers on the Cisco WiSM. After the conversion has been completed, add the SSC key–hash to the second controller on the Cisco WiSM by copying the SSC key–hash from the first controller to the second controller. In order to copy the SSC key–hash, open the AP Policies page of the controller GUI (**Security > AAA > AP Policies**), and copy the SSC key–hash from the SHA1 Key Hash column under AP Authorization List . Then, with the GUI of the second controller, open the same page and paste the key–hash into the SHA1 Key Hash field under Add AP to Authorization List. If you have more than one Cisco WiSM, use WCS to push the SSC key–hash to all the other controllers.
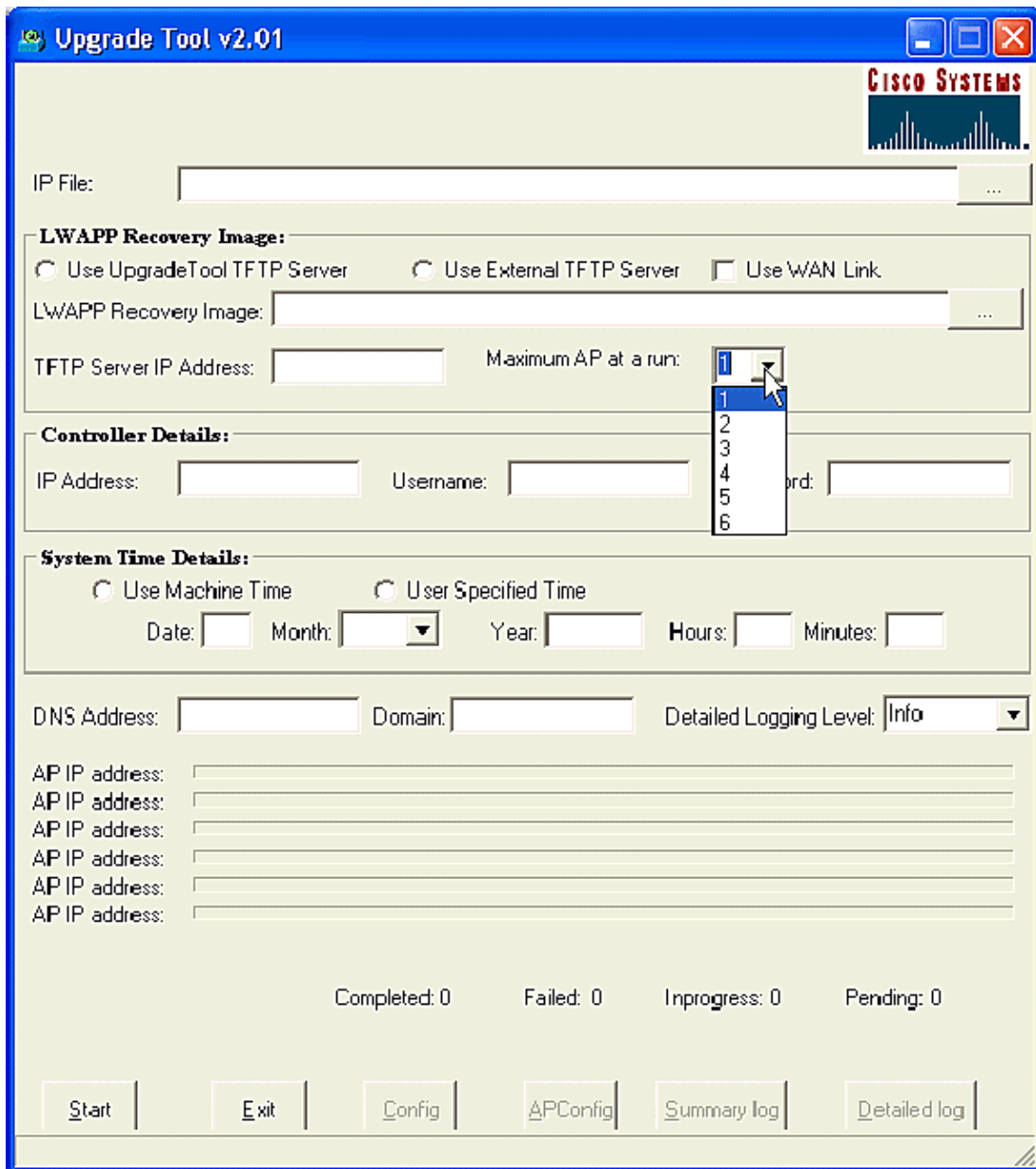
Refer to the Release Notes for Cisco Aironet 1130AG, 1200, 1230AG, and 1240AG Series Access Points for Cisco IOS Release 12.3(7)JX for details.

Q. I have converted my access point to lightweight mode, but I need to convert it back to autonomous mode. Is it possible?

A. Yes, you can convert autonomous APs that you have converted to lightweight mode back to autonomous mode. Complete the steps in the *Converting a Lightweight Access Point Back to Autonomous Mode* section of Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.

Q. How many access points can be converted via the upgrade tool at one time?

A. With the latest 2.01 version of the tool, you can upgrade a maximum of six APs at a time.

Q. I have converted my AP to Lightweight AP Protocol (LWAPP), but the AP does not register with the controller. I get the message "`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP.`" What causes this problem?

A. This error means that the X.509 digital certificates are not valid. It might be that you are experiencing Cisco bug ID CSCsd42296 (registered customers only) . The workaround for this issue is to reset the APs to the factory defaults.

Another possibility is that the self–signed certificate (SSC) is not registered at the WLC. Manual addition of the SSC at the controller can be necessary. Refer to Self–Signed Certificate Manual Addition to the Controller for LWAPP–Converted APs for the procedure.

Q. Can I configure a Cisco IOS Software–based AP as a workgroup bridge and associate with Lightweight AP Protocol (LWAPP)–based APs?

A. You can configure an access point to operate as a workgroup bridge so that it can provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the workgroup bridge access point. When you configure the access point to operate as a workgroup bridge and connect to a Cisco Unified network, it can provide wireless connectivity to wired clients that are connected by Ethernet to the workgroup bridge access point. For example, if you need to provide wireless connectivity for a group of wired devices, you can connect the devices to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge.

The document Workgroup Bridges in a Cisco Unified Wireless Network Configuration Example provides a configuration example.

Q. Can a wireless client roam between LWAPP APs and autonomous APs?

A. No, roaming between LAPs and autonomous APs is NOT supported. The reason is that, when connected to LWAPP APs, traffic is passed through an LWAPP tunnel. Since there is no mobility tunnel between the Wireless LAN Controller and autonomous APs, the roam does not work.

Q. What antenna options are available with the different models of Cisco Aironet 1000 Series LAPs?

A. The 1000 Series LAP enclosure contains:

- One IEEE 802.11a or one 802.11b/g radio antenna
- Four high−gain internal antennas (two 802.11a and two 802.11b/g)

You can enable or disable these antennas independently in order to produce a 180−degree sectorized or 360−degree omnidirectional coverage area. Some of the 1000 Series LAPs can also use external antennas. The 1000 Series LAPs come in three models:

- 1010 LAP
- 1020 LAP
- 1030 LAP

These are the available antenna options:

- 1010 LAP:

  - Four high−gain internal antennas
  - No external antenna adapters
- 1020 LAP:

  - Four high−gain internal antennas
  - One 5−GHz external antenna adapter
  - Two 2.4−GHz external antenna adapters
- 1030 LAP (remote−edge LAP):

  - Four high−gain internal antennas
  - One 5−GHz external antenna adapter
  - Two 2.4−GHz external antenna adapters

A. External-Antenna Model   B. Internal-Antenna Model

Note: The 1000 Series LAPs must use the factory–supplied internal or external antennas in order to avoid a violation of FCC requirements and to avoid a void of the user authority to operate the equipment.

Q. What power options are available for the Cisco Aironet 1000 Series LAPs?

A. The Aironet 1000 Series LAP can receive power from an external 110 through 220 VAC–to–48 VDC power supply or from Power over Ethernet equipment. The external power supply (AIR–PWR–1000) plugs in to a secure 110 through 220 VAC electrical outlet. The converter produces the required 48 VDC output for the 1000 Series LAP. The converter output feeds into the side of the 1000 Series LAP through a 48 VDC jack.

Note: You can order the AIR–PWR–1000 external power supply with country–specific electrical outlet power cords. Contact Cisco when you order in order to receive the correct power cord.

Q. Can I Telnet/SSH into an LWAPP based access point?

A. In Wireless LAN Controller release 5.0 and later, the controller supports the use of Telnet or Secure Shell (SSH) protocols to troubleshoot lightweight access points. You can use these protocols in order to make debugging easier, especially when the access point is unable to connect to the controller. You can configure Telnet and SSH support only through the controller CLI.

In order to enable Telnet or SSH connectivity on an access point, use the **config ap {telnet | ssh}** command. The Cisco lightweight access point associates with this Cisco Wireless LAN controller for all network operation and in the event of a hardware reset.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Examples

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

Q. How to configure global credentials for access points. What are the default user name and password in release 5.0?

A. Cisco IOS access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non–privileged mode and execute show and debug commands, which poses a security threat. The default enable password must be changed in order to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

In the controller software prior to release 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In controller software release 5.0, you can set a global use rname, password, and enable password that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.

For information on how to configure the global credentials of the AP, refer to Configuring Global Credentials for Access Points.

Q. I have Wireless LAN Controller (WLC) 2006 and access point (AP) 1242 with firmware version 3.2.78.0. I have issues with access points that connect to it and I receive these error messages: "lwapp_clinet_error;not receive read response(3). Lwapp_image_broc;unable to open TAR file"

A. AP 1242s are converted Lightweight Access Point Protocol (LWAPP) APs. Once you convert and try to use them, they try to search for the controller in order to join it. If the APs do not find the controller, then this type of message appears on the console. But in this case the controller has a firmware version of 3.2.78.0 which is not compatible to work with upgraded APs. You need to have firmware version 3.2.116.21 in order to work with upgraded APs. Once the controller firmware is upgraded, these APs join the controller and start to function.

Q. Clients show a MAC address of 00:17:0f:37:65:c4 when attached to an access point, but the access point shows that is has a base Radio MAC address of 00:17:0f:37:65:c0. Why does the client show a different MAC than the access point? Is there a way to determine which MAC address the device registers if I have two access points with very close MAC addresses?

A. If you look at an access point in detail mode, you can see that it has a base Radio MAC address and a FastEthernet MAC address. In addition, that is the base Radio MAC address that changes with the WLAN. The client actually sees the BSSID in the form of a MAC address.

Q. I have an existing wireless network (autonomous APs) with an access−point that is configured as a repeater. This network is to be migrated to a LWAPP wireless network. Can I use the LWAPP APs as repeaters?

A. LWAPP APs must join a controller, and they do not support a repeater mode since they all have to have some connectivity to the controller first. Cisco autonomous APs can be configured as repeaters, but due to the reduction in effective bandwidth available to end clients, repeaters are not the most highly recommended configuration. While any Cisco Aironet AP or LAP model can be used in either LWAPP or autonomous mode, in order to make that change, a software reimage is required. This is particularly complex when it goes from autonomous to LWAPP, so directly, no, an AIR−LAP1232AG−A−K9 does not natively support the repeater mode. It could be loaded with autonomous software and be made to support repeater mode, but that would involve a software change and a separate configuration.

Q. How many APs can WLCs support?

A. The number of APs supported per WLC depends on the model number:

- **2106** A standalone WLC that supports up to 6 APs with 8 Fast Ethernet interfaces.
- **4402** A standalone WLC that supports either 12, 25, or 50 APs.
- **4404** A standalone WLC that supports 100 APs.
- **5500** A standalone WLC that supports 12, 25, 50,100, or 250 access points for business−critical wireless services at locations of all sizes.
- **WLCM** A WLC module that is specifically designed for Cisco's Integrated Service Router (ISR) series. It's currently available in a 6, 8 or 12 AP version.
- **WS−C3750G** A WLC that supports either 25 or 50 APs that comes integrated with the Catalyst 3750 switch. The WLC's backplane connections appear as 2−Gig Ethernet ports that can be configured separately as dot1q trunks to provide connection into the 3750. Or the Gig ports can be link aggregated to provide a single EtherChannel connection to the 3750. Because the WLC is integrated directly, it has access to all of the advanced routing and switching features available in the 3750 stackable switch. This WLC is ideal for medium−sized offices or buildings. The `50 AP' version can scale up to 200 APs when four 3750s are stacked together as a virtual switch.
- **WiSM** A WLC module that is designed specifically for Cisco's Catalyst 6500 switch series. It supports up to 300 APs per module. Depending on the 6500 platform, multiple WISMs can be installed to offer significant scaling capabilities. The WiSM appears as a single aggregated link interface on the 6500 that can be configured as a dot1 trunk to provide connection into the 6500 backplane. This module is ideal for large buildings or campuses.

Q. What is the maximum number of client associations that an access points can support?

A. The maximum number of client associations that the access points can support depends on these factors:

- The maximum number of client associations differs for lightweight and Autonmous IOS access points.
- There might be a limit per radio and an overall limit per AP.

♦ AP hardware (16−MB APs have a lower limit than the 32−MB and higher APs).
For complete details on client association limits, refer to the *Client Association Limits* section
of the Cisco Wireless LAN Controller Configuration Guide, Release 7.0.

Q. Does the 1252 AP support bridging?

A. Yes, the bridging mode is supported on the 1252 series AP.

Q. Does the Lightweight AP Protocol (LWAPP) infrastructure support PPP over Ethernet (PPPoE) (PC client to a PPPoE server)?

A. No, the LWAPP infrastructure does not support PPPoE. The reason is that the PPPoE Ethertype is dropped at the controller.

Q. How can I manually reset the Cisco Aironet 1000 Series LAP?

A. You can reset the AP to the factory defaults through the wireless LAN (WLAN) controller (WLC). For the reset, the LAP should be registered to the WLC.

Complete these steps:

1. From the WLC GUI, click **Wireless**. The Wireless tab provides access to the Cisco WLAN Solution wireless network configuration.
2. Choose **Access Points > Cisco APs**, and then click **Detail** in order to navigate to the window for the specific AP.
3. Click **Clear Config** at the bottom of this window. This clears the configuration on the LAP and resets it to the factory defaults.

In order to reset the LAPs to the factory defaults with use of the command−line interface (CLI), issue the **clear ap−config** *ap−name* command from the WLC CLI.

Q. Where can I get more information on Cisco Aironet 1000 Series LAPs?

A. Refer to Cisco 1000 Series Lightweight Access Points − Q&A. The document provides answers to many questions that relate to the 1000 Series LAPs.

Q. Which Cisco devices support Lightweight AP Protocol (LWAPP) Layer 2 mode?

A. LWAPP Layer 2 mode is only supported on these Cisco devices:

♦ Cisco 4100 Series Wireless LAN Controller (WLC)
♦ Cisco 4400 Series WLC
♦ Cisco Aironet 1000 Series LAP

Q. I understand that the Cisco LAPs use a Vendor Class Identifier (VCI) string with DHCP option 43 for controller discovery. What is the VCI string value for Cisco LAPs?

A. Cisco Aironet 1000 Series APs use a string format for DHCP option 43, whereas the other Aironet APs use the type, length, value (TLV) format for DHCP option 43. You must program DHCP servers to return the option on the basis of the AP DHCP VCI string (DHCP

option 60). This table provides the VCI string values for the different LAPs:

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

Q. What is the significance of the type length value (TLV) block values with respect to DHCP option 43? How is the TLV value calculated?

A. DHCP option 43 can be enabled on the DHCP server of the Cisco IOS router using this command:

```
Option 43 hex <string>
```

The hexadecimal string in this command is assembled by concatenating the TLV values for the option 43 sub−option.

Type + Length + Value

- **Type** is always the sub−option code 0xf1.
- **Length** is the number of controller management IP addresses times 4 in hex.
- **Value** is the IP address of the controller listed sequentially in hex.

For example, assume that there are two controllers with management interface IP addresses 10.126.126.2 and 10.127.127.2:

- The type is 0xf1.
- The length is 2 * 4 = 8 = 0x08.
- The IP addresses translate to 0a7e7e02 (10.126.126.2) and 0a7f7f02 (10.127.127.2).
- Assembling the string then yields f1080a7e7e020a7f7f02. The IOS command then added to the DHCP scope is:

```
option 43 hex f1080a7e7e020a7f7f02
```

Q. Does the wireless LAN controller (WLC) support AP load balancing?

A. Yes, you can do AP load balancing on a WLC. Refer to Wireless LAN Controller (WLC) Troubleshoot FAQ for more information.

Q. How do I configure wireless LAN controller (WLC) failover for LAPs?

A. Refer to the WLAN Controller Failover for Lightweight Access Points Configuration Example for details on how to configure WLC failover.

Q. How can I disable the reset button on the APs after conversion from autonomous to lightweight mode?

A. You can disable the reset button on APs that you have converted to lightweight mode. The reset button is labeled "MODE" on the outside of the AP. Use this command in order to disable or enable the reset button on one or all converted APs that are associated to a controller:

```
config ap reset-button {enable | disable} {ap-name | all}
```

The reset button on converted APs is enabled by default.

Q. Can I have a Lightweight AP Protocol (LWAPP)–capable AP connected across a WAN link from the wireless LAN controller (WLC)? If so, how does this work?

A. Yes, some LAPs support the feature called Remote–Edge AP (REAP). With this feature, you can have a LAP across a WAN link from the WLC to which the LAP connects. REAP mode enables a LAP to reside across a WAN link and still be able to communicate with the WLC and provide the functionality of a regular LAP. Refer to Remote–Edge AP (REAP) with Lightweight APs and Wireless LAN Controllers (WLCs) Configuration Example for a detailed example of this setup.

Note: REAP mode is supported only on the Cisco Aironet 1030 LAPs at this point. The REAP functionality will be included on a broader range of LAPs in the future.

Q. Do we still have the same WAN restraints on monitor mode APs as we do with regular APs and H–REAP APs? That is, do we require a 100ms or better RTD between the controller and a monitor mode AP?

A. No, monitor mode AP does not have the 100 ms restriction because there is no client association, which is the reason for the restriction. The 100 ms latency limitation was created out of varied, and often stringent, client authorization requirements, which is why both local mode and H–REAP APs have identical latency limitations. Obviously, monitor mode APs do not have the same client limitations.

Q. My WLC version is 3.2. It is configured for Layer 3 Lightweight Access Point Protocol (LWAPP). The MTU for the network between this WLC and my lightweight access point (LAP) is configured as 900 bytes. My LWAPP AP is unable to join this WLC. What can be the reason for this?

A. The MTU configured in your scenario is 900 bytes. But an LWAPP Join request is larger than 1500 bytes. So, here LWAPP requires a fragment of the LWAPP Join request. The logic for all LWAPP APs is that the size of the first fragment is 1500 bytes (includes IP and UDP header) and the second fragment is 54 bytes (includes IP and UDP header). If the network between LWAPP APs and the WLC has an MTU size less than 1500 (such as VPN, GRE, MPLS, and so forth) as in your case, WLC cannot handle the LWAPP Join request. Therefore, the LWAPP is not able to join the controller.

Upgrade your controller to version 4.0 in order to handle this situation. This version is able to handle Layer 3 fragments. Refer to Cisco bug ID CSCsd94967 (registered customers only) for

more information on this issue.

Q. I have a WLC that I got from Singapore. With this WLC, my intention was to have a remote office connect to it (REAP) for wireless connectivity. I have offices in other countries. However, I receive regulatory domain error messages from the Singapore WLC. Is there a way to force the WLC to accept access points (APs) with different regulatory domains? The error message I receive is: `"AP 'AP_NAME' is unable to associate. The Regulatory Domain configured on it '-R' does not match the Controller 'A.B.C.D' country code 'SG – Singapore"`

A. The WLC supports only one regulatory domain. Therefore, a WLC that uses regulatory domain −A can only be used with APs that use regulatory domain −A (and so on). In this case, the WLC is set to −SG for Singapore, so it only supports APs in the Singapore regulatory domain.

When you purchase APs and WLCs, ensure that they share the same regulatory domain. Only then can the APs register with the WLC.

Multiple country code support With WLC version 4.1.171.0 and later, mulitple country code support is introduced with WLCs. With release 4.1.171.0 and later, you can configure up to 20 country codes per controller. Support for multiple country codes enables you to manage access points in various countries from a single controller. This feature is not supported for use with Cisco Aironet mesh access points.

Q. What are the different modes in which a lightweight access point (LAP) can operate?

A. An LAP can operate in any of these modes:

- ♦ **Local mode** This is the default mode of operation. When an LAP is placed into local mode, the AP will transmit on the normally assigned channel. However, the AP also monitors all other channels in the band over a period of 180 seconds to scan each of the other channels for 60ms during the non−transmit time. During this time, the AP performs noise floor measurements, measures interference, and scans for IDS events.
- ♦ **REAP mode** Remote Edge Access Point (REAP) mode enables an LAP to reside across a WAN link and still be able to communicate with the WLC and provide the functionality of a regular LAP. REAP mode is supported only on the 1030 LAPs.
- ♦ **H−REAP Mode** H−REAP is a wireless solution for branch office and remote office deployments. H−REAP enables customers to configure and control access points (APs) in a branch or remote office from the corporate office through a WAN link without the need to deploy a controller in each office. H−REAPs can switch client data traffic locally and perform client authentication locally when the connection to the controller is lost. When connected to the controller, H−REAPs can also tunnel traffic back to the controller.
- ♦ **Monitor mode** Monitor mode is a feature designed to allow specified LWAPP−enabled APs to exclude themselves from handling data traffic between clients and the infrastructure. They instead act as dedicated sensors for location based services (LBS), rogue access point detection, and intrusion detection (IDS). When APs are in Monitor mode they cannot serve clients and continuously cycle through all

configured channels listening to each channel for approximately 60 ms.

Note: From the controller release 5.0, LWAPPs can also be configured in Location Optimized Monitor Mode (LOMM), which optimizes the monitoring and location calculation of RFID tags. For more information on this mode, refer to Cisco Unified Wireless Network Software Release 5.0.

Note: With controller release 5.2, the **Location Optimized Monitor Mode (LOMM)** section has been renamed **Tracking Optimization**, and the **LOMM Enabled** drop−down box has been renamed **Enable Tracking Optimization**.

Note: For more information on how to configure Tracking Optimization, read the Optimizing RFID Tracking on Access Points section.

- ♦ **Rogue detector mode** LAPs that operate in Rogue Detector mode monitor the rogue APs. They do not transmit or contain rogue APs. The idea is that the rogue detector should be able to see all the VLANs in the network since rogue APs can be connected to any of the VLANs in the network (thus we connect it to a trunk port). The switch sends all the rogue AP/Client MAC address lists to the Rogue Detector (RD). The RD then forwards those up to the WLC in order to compare with the MACs of clients that the WLC APs have heard over the air. If MACs match, then the WLC knows the rogue AP to which those clients are connected is on the wired network.
- ♦ **Sniffer mode** An LWAPP that operates in Sniffer mode functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs Airopeek. These packets contain information on timestamp, signal strength, packet size and so on. The Sniffer feature can be enabled only if you run Airopeek, which is a third−party network analyzer software that supports decoding of data packets.
- ♦ **Bridge Mode** Bridge mode is used when the access points are setup in a mesh environment and used to bridge between each other.

Q. How do I change the mode on a Lightweight Access Point?

A. In order to change the mode of a Lightweight Access Point, complete these steps.

1. From the WLC GUI, choose **Wireless > Access Points > All APs**, and select the AP for which the mode needs to be changed from the list of registered APs.
2. The **All APs > Details for AP** page appears. On the **General** tab of this page, select the **AP Mode** from the drop−down menu, as shown:

All APs > Details for AP1130

General | Credentials | Interfaces | High Availability | Inventory | Advanced

General

AP Name	AP1130
Location	default location
AP MAC Address	00:16:c7:a0:ab:3e
Base Radio MAC	00:15:c7:ab:55:90
Status	Enable
AP Mode	local
Operational Status	
Port Number	

AP Mode dropdown: local / H-REAP / monitor / Rogue Detector / Sniffer / Bridge

Versions

Software Version	6.0.182.0
Boot Version	12.3.7.1
IOS Version	12.4(21a)JA
Mini IOS Version	3.0.51.0

IP Config

IP Address	10.77.244.221
Static IP	☑
Static IP	10.77.244.221
Netmask	255.255.255.224
Gateway	10.77.244.193
² DNS IP Address	0.0.0.0
Domain Name	

Time Statistics

UP Time	0 d, 00 h 11 m 28 s
Controller Associated Time	0 d, 00 h 01 m 41 s
Controller Association Latency	0 d, 00 h 00 m 14 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

Q. I have newly installed LAP−1131AG access points that have been primed to a particular controller. My controller version is 4.0.155.5. When I boot them up with the same Wireless LAN Controller (WLC) to which they are primed, they eventually turn light green. As per the documentation, this light green on the status LED means that they are connected to the WLC. But I could not find this access point in the access point list of the WLC. Why is this? Did the Lightweight Access Point Protocol (LWAPP) become associated?

A. If the access point is primed to a WLC at Layer 3 but cannot get an IP address during startup, then the status LED of the WLC turns to light green and does not go into the search and reboot sequence until it gets an IP address from DHCP.

So, in such scenarios, the status LED turning green does not indicate that the LWAPP is registered with the controller. After the access points are able to get their DHCP addresses, they search for the WLC and if not found, go through a reboot process and proceed as expected. There is a bug associated with this.

Refer to Cisco bug ID CSCsf10580 (registered customers only) for more information.

Q. What do the LEDs on the LAP indicate?

A. This is a link to a short video which explains how to interpret the LEDs on a 1130AG Lightweight AP:

Q. What is the difference between Roof–top Access Points (RAPs) and Pole–top Access Points (PAPs) as modes of lightweight Mesh Access Points (MAPs)?

A. These are the modes that the outdoor MAPs can operate as part of the mesh network. The mesh networking solution, which is part of the Cisco Unified Wireless Network Solution, enables two or more Cisco Aironet Lightweight MAPs to communicate with each other over one or more wireless hops to join multiple LANs or to extend 802.11b wireless coverage.

These access points are used as part of the mesh network and operate in two modes:

1. RAP
2. PAP

RAP Cisco MAPs that operate in RAP mode are the parent node to any bridging or mesh network and connect a bridge or mesh network to the wired network. Therefore, there can only be one RAP for any bridged or mesh network segment. In a mesh network, Cisco MAPs are configured, monitored, and operated from and through any Cisco WLAN controller (WLC) deployed. Any MAP that has the wired connection to the WLC assumes the role of RAP. This RAP uses the backhaul wireless interface to communicate with neighboring PAPs.

PAP Cisco MAPs that operate in PAP mode have no wired connection to a Cisco WLC. They can be completely wireless and support clients that communicate with other PAPs or RAPs, or they can be used to connect to peripheral devices or a wired network. The Ethernet port is disabled by default for security reasons, but you should enable it for PAPs.

Refer the Zero Touch Configuration section of the Cisco Mesh Networking Solution Deployment Guide for more information on how a MAP assumes the role of RAP and PAP.

Q. How do you interpret the radiation pattern of the 1000 Series Lightweight Access Point (LAP) Antennas?

A. Azimuth diagrams are usually with the device/antenna in normal operating orientation (vertical, top up, in the center of the diagram for omni; horizontal, mount at the center, forward direction towards "0" on the diagram). The A side is most likely forward and represented at the 0 mark for azimuth, and the 90 mark for elevation. The B side is represented at the 180 mark for azimuth, and 270 for elevation. The pattern does not change in free–space if the unit is inverted. But the immediate surfaces can cause reflection/absorbtion and can alter the pattern. Metallic objects near the radiators (within ~2 wavelengths or so) can also distort the pattern significantly. The Cisco Aironet Antenna Reference Guide has more information. The 1000 Series Antennas are explained in the last section of the document.

Q. Can we restrict which APs join a controller? I see the SECURITY/AAA/AP Policies page, where you can authorize APs against the AAA or certificate. I am able to add an AP to the Authorization List, but do these things restrict only my Authorization list of APs to join the controller?

A. No, controllers handle APs on a first come, first serve basis. You possibly can play with

the primary, secondary, and tertiary fields to increase the odds on AP connections to your preference.

Q. With LWAPP, is it possible to determine the SSIDs an AP has on an individual AP basis? What is required to be able to have specific APs in a zone that use a unique SSID, and all the rest that use another set of SSIDs?

A. With the WLAN override option, you can choose which SSIDs an AP offers. Controllers support only up to 16 SSIDs each, so you can only choose from among the supported 16. This is done on a per–AP basis.

Q. When I enable some LWAPP commands on my LAP, I get an error that says the command is disabled. Why is this?

```
AccessPoint#clear lwapp ap controller ip addressERROR!!! Command is disabled.
```

A. Once your AP has successfully joined a controller, the LWAPP commands are disabled. In order to enable LWAPP commands again, you must set the username/password of the AP from the controller CLI with the **config ap username <name> password <pwd> <cisco–ap>/all** command. Once that is done, you can do a **clear lwapp private–config** in the AP CLI to allow you to manually re–issue the AP LWAPP configuration commands.

Note: If you are running WLC version 5.0 and later, use this command to set the username and password on the AP:

```
config ap mgmtuser add username AP_username
password AP_password secret secret {all | Cisco_AP}
```

Q. When two APs are on the same channel and can see each other, what are the implications (for roaming throughput, etc.) over the use of four channels instead of three? How do the APs react in such a situation and how does a client react?

A. Whether APs are on the same channel or not, it does not particularly impact client roaming. What does matter is sufficient cell overlap such that clients can make smooth transitions from the coverage area of one AP to the next. The intent of a move from a three–channel design to a four–channel design is to increase design flexibility (because of the extra channel). This approach is shortsighted because, while you add a bit of deployment flexibility (since you have another channel), you actually increase the amount of co–channel interference. What you might gain in design flexibility with the four–channel approach, you lose in the added co–channel interference. Bottom line: do not use a four–channel design.

Q. Can we control when clients roam? Can we let the client roam solely based on the signal strength on an individual AP basis and for all client adapters?

A. Today, roaming is always a function of the client, and the choice to roam or not is implemented differently in various clients. Directed Roaming is a part of CCX, but it is an optional feature and is not used today.

Q. Are there any specific requirements or recommendations for a WAN link that is implemented between REAP/HREAP AP at the remote site and WLC at the main site?

A. These are some of the main factors to be considered for the WAN link:

♦ Ensure that the bandwidth of the WAN link is at least 128kbps.
♦ Ensure that the latency or round−trip delay between the two sites across the WAN link is not more than 300ms because more than a 300ms delay can create authentication problems to the client, especially when central authentication is implemented.

Q. I had a network shut down for a few hours, due to which the LAPs lost communication with WLCs. After the network came back up, the LAPs took the IP address from the DHCP server, even though these APs are configured with a static IP address. In the "`show ap config general <ap-name>`" it shows as "`Fallback IP Address.`" Why does this happen?

A. The LAP tries to associate with the WLC up to 20 times with LWAPP discovery messages. In case it is not able connect, it tries to obtain a new IP address through DHCP. If the LAP is able to get one IP address from the DHCP server, this IP address is the active one, and the statically assigned IP address is used for fallback. The idea behind this is that in case the LAPs are moved to a different VLAN (for example, to a another building), they are able to retrieve an IP address and join a WLC. This behavior is explained in bug CSCse66714. You must upgrade the WLC to software Version 4.0.206.0.

Q. Is it mandatory to configure a bridge group name for a mesh network?

A. A bridge group name (BGN) can be used to logically group the APs in the mesh. Although by default, the APs come with a null value BGN to allow association, we recommend that you set a BGN. You can make this configuration change through the CLI or GUI with this command:

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

Note: BGNs can be a maximum of ten characters. If you enter more than 10 characters into the BGN field on the controller GUI mesh access point configuration page, it generates an error message. An error also appears when you configure this parameter through the **config ap bridgegroupname set groupname Cisco_MAP** CLI command or WCS (CSCsk64812).

When you configure BGN on a live network, ensure that you configure from the farthest MAP and work your way back to the RAP. This is very important because you can strand a child MAP that cannot associate with a parent, which can have an updated BGN. Use different BGNs to logically group different parts of your network. This is useful in situations where you have RAPs within the same RF area and you want to keep segments of your mesh separated.

If you want to add a new AP to a live network, you must pre−configure the BGN on the new AP. If you bring up the mesh network from the scratch with new, out−of−the−box APs, the BGN is preset in the APs to a NULL value. APs join in a new network with this default value

of the BGN. You can verify the BGN of an AP with this command:

```
show ap config general Cisco AP
```

Q. What happens if the BGN is not configured correctly?

A. If the AP is wrongly provisioned with a bridgegroupname other than the one for which it is intended, dependent upon the network design, this AP can or cannot be able to reach out and find its correct sector or tree. If it cannot reach a compatible sector, it can become stranded. In order to recover such a stranded AP, the concept of default bridgegroupname has been introduced. The basic idea is that an AP, which is unable to connect to any other AP with its configured bridgegroupname, attempts to connect with the bridgegroupname of default.

This is the algorithm used to detect this strand condition and recovery:

1. Passively scan and find all neighbor nodes, regardless of their bridgegroupname.
2. The AP attempts to connect to the neighbors that are heard with their own bridgegroupname with Adaptive Wireless Path Protocol (AWPP).
3. If Step 2 fails, attempt to connect with the default bridgegroupname with AWPP.
4. For each failed attempt of Step 3, exclusion–list the neighbor and attempt to connect the next best neighbor.
5. If the AP fails to connect with all neighbors in Step 4, reboot the AP.
6. If connected with default bridgegroupname for 30 minutes, re–scan all channels and attempt to connect with the correct bridgegroupname.

Note: When an AP is able to connect with the default bridgegroupname, the parent node reports the AP as a default child/node/neighbor entry on the WLAN controller so that a network administrator is aware of the stranded AP. Such an AP cannot accept any client or other mesh nodes as its children, nor can it pass any data traffic through.

Q. Can a LAP 1030 bridge to any other bridge models? Also can a LAP 1020 support bridging?

A. The LAP 1020 model does not support bridging. The LAP 1030 supports bridging (one hop) to another LAP 1030 but not to a BR1310, BR1400, or LAP 1500 at this time.

Q. Is it possible to set up wireless bridging between LAP APs? I would like one radio on my non–wired LAPs to perform bridging back to the wired root bridge LAPs (LAP connected to a WLC). Is this possible?

A. No. This cannot be done on LAP APs. Mesh APs can perform basic point–to–point bridging in a Cisco Unified Wireless Network. The only other bridging possible is through IOS APs in WGB (Workgroup Bridge) mode. These IOS APs act as clients (with wired devices behind them) to a LAP AP. But wireless clients cannot connect to these IOS APs.

Q. I have a LAP 1131, and this access point is successfully registered to the Wireless LAN Controllers. When I connect the access point without the power injector, the radios are up (LED status is green), but when I connect the AP with the power injector, the radios are down (LED status is orange). How I can resolve this issue?

A. This issue can be due to incorrectly configured Power over Ethernet (POE) parameters;

complete these steps in order to resolve this issue:

1. Click **Wireless** in order to access these parameters.
2. Click the **Detail** link of the desired access point. The new parameters appear on the All APs > Details page under the POE settings.
3. On the APs > Details page of the access point for the POE settings, click **Power Injector State**, and choose **Installed**.
4. Check the check box to enable the Power Injector State for the access point. This parameter is required if the attached switch does not support IPM and a power injector is used. This parameter is not required if the attached switch supports IPM.

Q. In autonomous APs, Public Secure Packet Forwarding (PSPF) is used to avoid client devices associated to this AP from inadvertently sharing files with other client devices on the wireless network. Is there any equivalent feature in Lightweight APs?

A. The feature or the mode that performs the similar function of PSPF in lightweight architecture is called peer–to–peer blocking mode. Peer–to–peer blocking mode is actually available with the controllers that manage the LAP.

If this mode is disabled on the controller (which is the default setting), it allows the wireless clients to communicate with each other through the controller. If the mode is enabled, it blocks the communication between clients through the controller.

It only works among the APs that have joined to the same controller. When enabled, this mode does not block wireless clients terminated on one controller from the ability to get to wireless clients terminated on a different controller, even in the same mobility group.

Q. Can a LAP AP handle SNMP messages like an IOS AP?

A. The LAP APs cannot handle SNMP messages on their own. In order to handle SNMP messages, you should configure an SNMP community on the WLC to which the LAP is registered. All the AP information is managed by the WLC.

Related Information

- **Wireless LAN Controller (WLC) Troubleshoot FAQ**
- **Cisco Wireless LAN Controller Modules**
- **Cisco Wireless LAN Controller (WLC) FAQ**
- **Cisco Wireless LAN Controller Configuration Guide, Release 3.2**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Technical Support & Documentation – Cisco Systems**