

Cisco Internal - WLAN - NIP 9800

**.**

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

# Contents

[Contents 2](#_Toc256000000)

[List of Figures 4](#_Toc256000001)

[List of Tables 5](#_Toc256000002)

[About This Document 6](#_Toc256000003)

[History 6](#_Toc256000004)

[Review 6](#_Toc256000005)

[Document Conventions 6](#_Toc256000006)

[1 Introduction 7](#_Toc256000007)

[1.1 Preface 7](#_Toc256000008)

[1.2 Audience 7](#_Toc256000009)

[1.3 Scope 7](#_Toc256000010)

[1.4 Assumptions 7](#_Toc256000011)

[1.5 Related Documents 8](#_Toc256000012)

[1.6 Project Contact List 8](#_Toc256000013)

[2 Project Overview 9](#_Toc256000014)

[2.1 High Level Project Overview 9](#_Toc256000015)

[2.2 Network Topology Diagram 9](#_Toc256000016)

[2.2.1 Logical Network Topology 9](#_Toc256000017)

[3 Network Information 10](#_Toc256000018)

[3.1 Network Closets 10](#_Toc256000019)

[3.2 IP Addressing 10](#_Toc256000020)

[3.3 Naming Conventions 10](#_Toc256000021)

[3.3.1 WLAN Controller IP Addressing 10](#_Toc256000022)

[3.3.2 Mobility Services Engine (CMX) IP Addressing 11](#_Toc256000023)

[3.3.3 Access Point IP Addressing 11](#_Toc256000024)

[3.3.4 Wireless Client IP Addressing 12](#_Toc256000025)

[3.4 Hardware/Software Releases 12](#_Toc256000026)

[4 Network Implementation Plan 14](#_Toc256000027)

[4.1 Configuration of Core Switches 14](#_Toc256000028)

[4.2 Configuration of Access Switches 17](#_Toc256000029)

[4.3 Implementation Tasks for Foreign WLC 9800-40 17](#_Toc256000030)

[4.3.1 Physical Connections 17](#_Toc256000031)

[4.3.2 Initial Configuration 19](#_Toc256000032)

[4.4 Software Installation and Upgrade 21](#_Toc256000033)

[4.5 Catalyst 9800 Configuration Model 22](#_Toc256000034)

[4.5.1 Profiles 22](#_Toc256000035)

[4.5.1.1 WLAN Profile 23](#_Toc256000036)

[4.5.1.2 Policy Profile 23](#_Toc256000037)

[4.5.1.3 AP Join Profile 24](#_Toc256000038)

[4.5.1.4 RF Profile 25](#_Toc256000039)

[4.5.2 Tags 26](#_Toc256000040)

[4.5.2.1 Policy Tag 27](#_Toc256000041)

[4.5.2.2 Site Tag 27](#_Toc256000042)

[4.5.2.3 RF Tag 28](#_Toc256000043)

# List of Figures

[Figure 1 Cisco Catalyst 9800-40 Front Panel View 18](#_Toc256000084)

[Figure 2 System Configuration Dialog 19](#_Toc256000085)

[Figure 3 Software Version Checking 21](#_Toc256000086)

[Figure 4 Software Version Checking 21](#_Toc256000087)

[Figure 5 Cisco Internal Campus Tags 22](#_Toc256000088)

[Figure 6 Composition of Tags 23](#_Toc256000089)

[Figure 7 Policy Tag 24](#_Toc256000090)

[Figure 8 RF Tag 25](#_Toc256000091)

[Figure 9 Combining All the Tags 27](#_Toc256000092)

[Figure 10 Assigning Tags to Form AP Groupings 28](#_Toc256000093)

[Figure 11 Cisco 8540 Wireless LAN Controller Rear Panel View 29](#_Toc256000094)

[Figure 12 Rear Panel SFP Distribution Ports and LEDs 30](#_Toc256000095)

[Figure 13 Cisco WLC High Availability Physical Connection 31](#_Toc256000096)

[Figure 14 Cisco WLC High Availability Logical View 31](#_Toc256000097)

[Figure 15 WLC Login Page 34](#_Toc256000098)

[Figure 16 ANC-WLC1 Boot-up Logs 36](#_Toc256000099)

[Figure 17 ANC-WLC2 Boot-up Logs 36](#_Toc256000100)

[Figure 18 ANC-WLC2 Boot-up Logs after Downloading XML Configuration from Active WLC 36](#_Toc256000101)

[Figure 19 Connecting CMX and DNA Spaces- CMX Login Window 48](#_Toc256000102)

[Figure 20 Connecting CMX and DNA Spaces - Manage>Notifications 48](#_Toc256000103)

[Figure 21 Connecting CMX and DNA Spaces- Create New Notifications 49](#_Toc256000104)

[Figure 22 Connecting CMX and DNA Spaces- DNA Spaces Dashboard 49](#_Toc256000105)

[Figure 23 Connecting CMX and DNA Spaces- Connecting your wireless network 50](#_Toc256000106)

[Figure 24 Connecting CMX and DNA Spaces- Automatic Sync 50](#_Toc256000107)

[Figure 25 Connecting CMX and DNA Spaces- Add CMX On-Prem-1 50](#_Toc256000108)

[Figure 26 Connecting CMX and DNA Spaces- Add CMX On-Prem-1 51](#_Toc256000109)

# List of Tables

[Table 1 Cisco Internal Site Locations 7](#_Toc256000110)

[Table 2 Assumptions 7](#_Toc256000111)

[Table 3 Related Documents 8](#_Toc256000112)

[Table 4 Cisco Internal Contacts 8](#_Toc256000113)

[Table 5 Partner Contacts 8](#_Toc256000114)

[Table 6 Cisco Contacts 8](#_Toc256000115)

[Table 7 Network Closet Information 10](#_Toc256000116)

[Table 8 WLAN Components Naming Conventions 10](#_Toc256000117)

[Table 9 DC1-WLC1 10](#_Toc256000118)

[Table 10 DC2-WLC2 10](#_Toc256000119)

[Table 11 ANC-WLC1 11](#_Toc256000120)

[Table 12 ANC-WLC2 11](#_Toc256000121)

[Table 13 DC1-LOC1 11](#_Toc256000122)

[Table 14 DC2-LOC1 11](#_Toc256000123)

[Table 15 Cisco Internal Access Point VLANs, Subnets, and DHCP Scope Parameters 11](#_Toc256000124)

[Table 16 Corporate VLANs and IP Subnets 12](#_Toc256000125)

[Table 17 Infrastructure IP Addresses 12](#_Toc256000126)

[Table 18 Domain Names 12](#_Toc256000127)

[Table 19 Recommended OS Version for WLAN Infrastructure Devices 12](#_Toc256000128)

[Table 20 WLC Physical Connectivity 17](#_Toc256000129)

[Table 21 Cisco Catalyst 9800-40 Wireless Controller Front Panel View Port Descriptions 18](#_Toc256000130)

[Table 22 Procedure for Initial Configuration 19](#_Toc256000131)

[Table 23 Install Mode versus Bundle Mode 21](#_Toc256000132)

[Table 24 Procedure for Installation and Upgrade 21](#_Toc256000133)

[Table 25 WLC Physical Connectivity 29](#_Toc256000134)

[Table 26 Cisco 8540 Wireless LAN Controller Rear Panel View Port Description 30](#_Toc256000135)

[Table 27 SFP Ports and LEDs 30](#_Toc256000136)

[Table 28 Initial Configuration of WLC 8540 using Setup Wizard 32](#_Toc256000137)

[Table 29 CIMC Port Configuration Commands 34](#_Toc256000138)

[Table 30 System Configuration Commands 37](#_Toc256000139)

[Table 31 NTP Configuration Commands 37](#_Toc256000140)

[Table 32 Mobility and Roaming Configuration Commands 37](#_Toc256000141)

[Table 33 Mobility and Roaming Configuration Commands 38](#_Toc256000142)

[Table 34 Security Configuration Commands 39](#_Toc256000143)

[Table 35 Guest Pre-Authentication Redirect ACL 40](#_Toc256000144)

[Table 36 Netflow Configuration Commands 42](#_Toc256000145)

[Table 37 Guest WLAN Configuration Commands 42](#_Toc256000146)

[Table 38 Local Mode APs - Antenna Gain Configuration 43](#_Toc256000147)

[Table 39 MSE Physical Connectivity 44](#_Toc256000148)

[Table 40 CMX Location - MSE Parameters 45](#_Toc256000149)

[Table 41 CMX MAC Address and Keys Configuration 46](#_Toc256000150)

# Introduction

## Preface

This *Network Implementation Plan* document builds upon the Cisco Internal HLD and LLD documents. The NIP document will provide the actual technology specific configurations which have been developed for Cisco Internal's environment. These configurations will be also served as a reference as the day 1 configuration for the Cisco Internal environment. This document was developed in collaboration with the following teams and organizations through a series of workshops and meetings:

* Cisco Internal's <Team Name>

## Audience

This document is intended for the following teams:

* Cisco Internal WLAN Manager
* Cisco Internal WLAN Manager
* Cisco Internal Operations Team

## Scope

The scope of this document is limited to the following:

* The BoM found in Appendix <Insert Appendix No.>
* The customer sites listed in the table below Cisco Internal Site Locations

Table 1 Cisco Internal Site Locations

|  |  |
| --- | --- |
| No. | Site Name |
| 1 | <Insert customer' site location> |
| 2 |  |
| 3 |  |

## Assumptions

The following assumptions have been made during the development of this document.

Table 2 Assumptions

|  |  |  |
| --- | --- | --- |
| No. | Assumption | Validated |
| 1 | All work detailed in the preparation and implementation guidelines complete. | Yes/No |
| 2 | All required network connectivity (as shown within the enclosed diagrams) is in place, operational and stable. | Yes/No |
| 3 | All software is at agreed go-live levels. | Yes/No |
| 4 | Internet links are assumed to have enough bandwidth capacity to handle the required throughput and enough NAT/PAT capacity to handle the required client session scales. | Yes/No |
| 5 | All access switches are assumed to have enough power budgets and port PoE+ capabilities to support the required number of connected APs, considering the AP model PoE+ requirements. | Yes/No |
| 6 | <Insert Assumptions related to project in this document> | Yes/No |

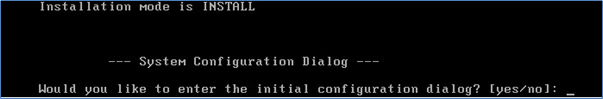
# Network Implementation Plan

## Implementation Tasks for Foreign WLC Cisco Router 9800 Initial Configuration

The Cisco Catalyst 9800 Wireless Controller (further referred to as Catalyst 9800) boots up similarly to any other Cisco router or switch running the IOS-XE software (see below), which may be familiar to the user.

The devices may have been switched on already, or an operator may have plugged in a terminal emulator to the console port and watched the device boot up.   
On completion of the boot process, the screen below should be displayed. Power up the device if not already done by pressing the switch next to the power supplies.

Figure 2 System Configuration Dialog



The following steps avoid the need to complete the Day 0 wizard.

Table 22 Procedure for Initial Configuration

|  |  |
| --- | --- |
| Step Number | Description of the Step |
| **Step 1** | Access the CLI of each Catalyst 9800 via the console port. |
| **Step 2** | Terminate the configuration wizard (this wizard is common to IOS-XE devices) by answering the questions:   * Would you like to enter the initial configuration dialog? [yes/no]: **no** * Would you like to terminate autoinstall? [yes]: **yes** |
| **Step 3** | Start configuration by typing the command:  conf t  Initially, there will be no password. |
| **Step 4** | Set the hostname on each Catalyst 9800 by typing the commands:  WLC(config)#hostname cisco  The command prompt text has been simplified for the sake of this document. |
| **Step 5** | Enter the config mode and add temporary login credentials using the command:  C9800(config)#username admin privilege 15 secret cisco123 |
| **Step 6** | Configure the service port OOB management interface by typing the command:   C9800#conf t  Enter configuration commands below, one per line and end with CNTL/Z.  C9800(config)# interface GigabitEthernet0  C9800(config)# vrf forwarding 192.1.1.1  C9800(config)# ip address 192.168.1.100 |
| **Step 7** | Configure a default route (or a more specific route) to reach the box:  C9800(config-if)# ip route vrf 192.1.1.1 0.0.0.0 0.0.0.0 192.168.1.1  C9800(config-if)# ip route 0.0.0.0 0.0.0.0 |
| **Step 8** | Configure the SVI for wireless management interface:  C9800(config)#int vlan 123  C9800(config-if)#ip address 192.1.1.1 23  C9800(config-if)#no shutdown |
| **Step 9** | Configure the interface Port-channel1 as trunk:  C9800(config-if)#interface Port-channel1  C9800(config-if)#switchport mode trunk  C9800(config-if)#switchport trunk allowed vlan 123  C9800(config-if)#shut  C9800(config-if)#no shut |
| **Step 10** | Add all the interfaces to Port-channel1 by typing the commands:  C9800(config-if)#interface range tenGigabitEthernet 0/0/0-3  C9800(config-if)#channel-group 1 mode on |
| **Step 11** | Disable the wireless network to configure the country code.  Type the command:  C9800(config)#ap dot11 5ghz shutdown  Answer the question that will appear:   * Disabling the 802.11a network may strand mesh APs. Are you sure you want to continue? (y/n)[y]: **y**   Type the command:  C9800(config)#ap dot11 24ghz shutdown  Answer the question that will appear:   * Disabling the 802.11b network may strand mesh APs. Are you sure you want to continue? (y/n)[y]: **y** |
| **Step 12** | Configure the AP country domain:  C9800(config)#ap country IN  Enter the country code (e.g. US, MX, IN) up to a maximum of 20 countries.  *This configuration will trigger the GUI to skip the DAY 0 flow as the Catalyst 9800 needs a country code to be operational.* |
| **Step 13** | Enable the wireless network to configure the country code:  C9800(config)#no ap dot11 5ghz shutdown  C9800(config)#no ap dot11 24ghz shutdown |
| **Step 14** | Specify the interface to be the wireless management interface:  C9800(config)#wireless management interface vlan 123  Verify certificate installation:  C9800#show wireless management trustpoint   * Trustpoint Name: CISCO\_IDEVID\_SUDI * Certificate Info: Available * Certificate Type: MIC * Private key Info: Available * FIPS suitability: Not Applicable |
| **Step 15** | Verify that you can ping the service management interface by entering:  https:// 192.1.1.1  Use the credentials you have entered earlier. Since the box has a country code configured, the GUI will skip DAY 0 page and you will get access to the main Dashboard for DAY 1 configuration. |