Cisco IP Phone 6861 Multiplatform Phones Wireless LAN Deployment Guide

The Cisco IP Phone 6861 Multiplatform Phones are adaptable for scenarios that require the ability to unplug the wired network connection and remain connected. The Wireless LAN capability enables communications in a WLAN-deployed working place or home.

This guide provides information and guidance to help you deploy the phone in a wireless LAN environment.

Revision History

Date	Comments
08/03/19	Initial version
08/06/19	Updated based on review comments

Contents

Table of Contents

WLAN Capability Overview

The Cisco IP Phone 6861 Multiplatform Phones extend collaboration to wireless network with 802.11 implementation. You can use the Cisco Unified Communication applications on the phone with either wired or wireless network.

With an enhancement on QoS control, the implementation of 802.11 permits time-sensitive applications, such as voice, to operate efficiently over wireless LAN (WLAN) deployment. These extensions provide bandwidth allocation ahead of a service if the AP supports it too, which guarantees the efficiency and good experience of communication for traffic over the air.

Since WLAN uses unlicensed spectrum, it may experience interference from other devices using the unlicensed spectrum. The proliferation of devices in the 2.4 GHz spectrum, such as Bluetooth headsets, Microwave ovens, and cordless consumer phones, means that the 2.4 GHz spectrum may contain more congestion than other spectrums. The 5 GHz spectrum has far fewer devices operating in this spectrum and is the preferred spectrum to operate the phone in order to take advantage of the 802.11a/n data rates available.

Despite the optimizations that Cisco has implemented in Cisco IP Phone 6861 Multiplatform Phones, we can’t guarantee uninterrupted communication in using the unlicensed spectrum, and there may be the possibility of voice gaps of up to several seconds during conversations. Adherence to these deployment guidelines will reduce the likelihood of these voice gaps being present, but there is always the possibility.

Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, the Cisco IP Phone 6861 Multiplatform Phone is not intended to be used as a medical device and should not be used to make clinical decisions.

Supported Frequencies and Channels

The following table lists the frequencies and channels that Cisco IP Phone 6861 Multiplatform Phones support.

Part Number	Description	Peak Antenna Gain	Frequency Ranges	Available Channels	Channel Set
CP-6861-3PW-CE-K9= CP-6861-3PW-NA-K9= CP-6861-3PW-UK-K9= CP-6861-3PW-AU-K9=	Cisco MPP Phone 6861	2.412-2.472GHz: 2.44 dBi	2.412 - 2.472 GHz	13	1-13
		5.150-5.350GHz: 0.53 dBi	5.180 - 5.240 GHz	4	36,40,44,48
		5.470-5.725GHz: 0.7 dBi	5.260 - 5.320 GHz	4	52,56,60,64
			5.500 - 5.700 GHz	11	100-144
			5.745 - 5.825 GHz	5	149,153,157,161,165

Requirements

Before deploying your phone, ensure that the requirements for the site and WLAN network are met.

Site Requirements

Before deploying the phone into a production environment, the site WLAN network deployment must be properly configured to accommodate more devices. Typically, there is less interference in the 5 GHz band and more non-overlapping channels, so 5 GHz is the preferred band for operation and even more highly recommended when the phone is to be used in a mission-critical environment.

The wireless LAN must be validated to ensure it meets the requirements to deploy the phone.

Signal

The signal coverage should be no lower than -67 dBm to ensure that the phone always has adequate signal.

Channel Utilization

Channel Utilization levels should be kept under 40%.

The phone converts the 0-255 scale value to a percentage, so 105 would equate to around 40% on the phone.

Noise

Noise levels should not exceed -92 dBm, which allows for a Signal to Noise Ratio (SNR) of 25 dB where a -67 dBm signal should be maintained.

Ensure that the upstream signal from the phone meets the access point's SNR for the transmitted data rate.

Packet Loss / Delay

Per voice guidelines, packet loss should not exceed 1%. Otherwise, the voice quality can be degraded significantly.

Jitter should be kept at the minimal (< 100 ms).

Retries

802.11 retransmission should be less than 20%.

Multipath

Multipath should be kept to the minimal to create nulls and reduce signal levels.

Number of allowed devices

The total number of connected devices to a given AP is no more than 10.

Separate SSID

We recommend that you put the phone in a separate SSID to guarantee voice traffic on the phone. Sharing the same SSID with other devices may impact phone calls on the phone when the other devices are using heavy network traffic. For voice deployments, it is suggested to use 802.11a/n for voice and use 802.11b/g/n for data.

Wireless LAN

The Cisco IP Phone 6861 Multiplatform Phones are recommended to work with the following Wireless LAN solutions:

- Mainstream AP for home use
- Cisco Autonomous Access Points
  - Minimum = 12.4(21a)JY
  - Recommended = 12.4(25d)JA2, 15.2(4)JB6, 15.3(3)JD

Protocols

The supported wireless LAN protocols include the following:

- 802.11a, b, d, e, g, h, i, n
- Wi-Fi MultiMedia (WMM)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)

Regulatory

World Mode (802.11d) allows a client to be used in different regions, where the client can adapt to use the channels and transmit powers advertised by the access point in the local environment.

The phone operates best when the access point is 802.11d-enabled. The AP can determine the channels and transmit powers per the local region.

Enable World Mode (802.11d) for the corresponding country where the access point is located.

Some 5 GHz channels are also used by radar technology, which requires that the 802.11 client and access point to be 802.11h-compliant to utilize those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

The Cisco IP Phone 6861 Multiplatform Phone will passively scan DFS channels first before engaging in active scans of those channels.

If 802.11d is not enabled, then the phone can attempt to connect to the access point using reduced transmit power.

Below are the countries and their 802.11d codes that the phone supports.

Argentina (AR)
Australia (AU)
Austria (AT)
Bahrain (BH)
Belgium (BE)
Brazil (BR)
Bulgaria (BG)
Canada (CA)
Chile (CL)
Colombia (CO)
Costa Rica (CR)
Croatia (HR)
Cyprus (CY)
Czech Republic (CZ)
Denmark (DK)
Dominican Republic (DO)
Ecuador (EC)
Egypt (EG)
Estonia (EE)
Finland (FI)
France (FR)
Germany (DE)
Gibraltar (GI)
Greece (GR)
Hong Kong (HK)
Hungary (HU)
Iceland (IS)
India (IN)
Ireland (IE)
Israel (IL)
Italy (IT)
Japan (JP)
Korea (KR)
Latvia (LV)
Liechtenstein (LI)
Lithuania (LT)
Luxembourg (LU)
Macau (MO)
Macedonia (MK)
Malaysia (MY)
Malta (MT)
Mexico (MX)
Monaco (MC)
Montenegro (ME)
Netherlands (NL)
New Zealand (NZ)
Nigeria (NG)
Norway (NO)
Oman (OM)
Panama (PA)
Paraguay (PY)
Peru (PE)
Philippines (PH)
Poland (PL)
Portugal (PT)
Puerto Rico (PR)
Romania (RO)
Russian Federation (RU)
Saudi Arabia (SA)
Serbia (RS)
Singapore (SG)
Slovakia (SK)
Slovenia (SI)
South Africa (ZA)
Spain (ES)
Sweden (SE)
Switzerland (CH)
Taiwan (TW)
Thailand (TH)
Turkey (TR)
Ukraine (UA)
United Arab Emirates (AE)
United Kingdom (GB)
United States (US)
Uruguay (UY)
Venezuela (VE)
Vietnam (VN)

Security

When deploying a wireless LAN, security is essential. The phone supports the following wireless security features.

- WLAN Authentication
  - WPA2-PSK (Pre-Shared key + AES encryption)
  - WPA-PSK (Pre-Shared key + TKIP encryption)
  - WPA2 (802.1x authentication + AES or TKIP encryption)

  - WPA (802.1x authentication + TKIP or AES encryption)
  - EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling)[1]
  - EAP-TLS (Extensible Authentication Protocol - Transport Layer Security))[1]
  - PEAP-GTC (Protected Extensible Authentication Protocol - Generic Token Card))[1]
  - PEAP-MSCHAPv2 (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol version 2))[1]
  - None

- WLAN Encryption
  - AES (Advanced Encryption Standard)
  - TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
  - WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

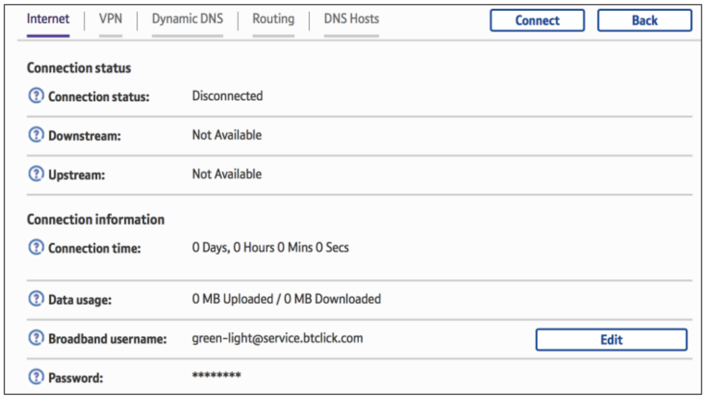
Note: An external authentication system is required.

Configure Wireless LAN

Configure Mainstream Home-Based AP

When configuring a mainstream home-based access point, ensure that:

1. You enable internet access as below picture shows. The internet connection could be set up via wideband user account on DSL or fiber link to external network.



Connection status

Connection status: Disconnected

Downstream: Not Available

Upstream: Not Available

Connection information

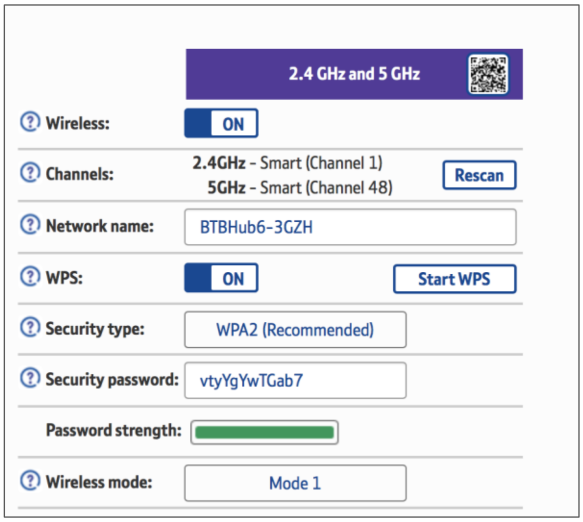
Connection time: 0 Days, 0 Hours 0 Mins 0 Secs

Data usage: 0 MB Uploaded / 0 MB Downloaded

Broadband username: green-light@service.btclick.com

Password: ********

2. You configure the local SSID and the secure mode for home/office usage as following picture shows.



Wireless: ON

Channels: 2.4GHz - Smart (Channel 1)
5GHz - Smart (Channel 48)

Network name: BTBHub6-3GZH

WPS: ON

Security type: WPA2 (Recommended)

Security password: vtyYgYwTGab7

Password strength: 🟩

Wireless mode: Mode 1

Cisco Autonomous Access Points

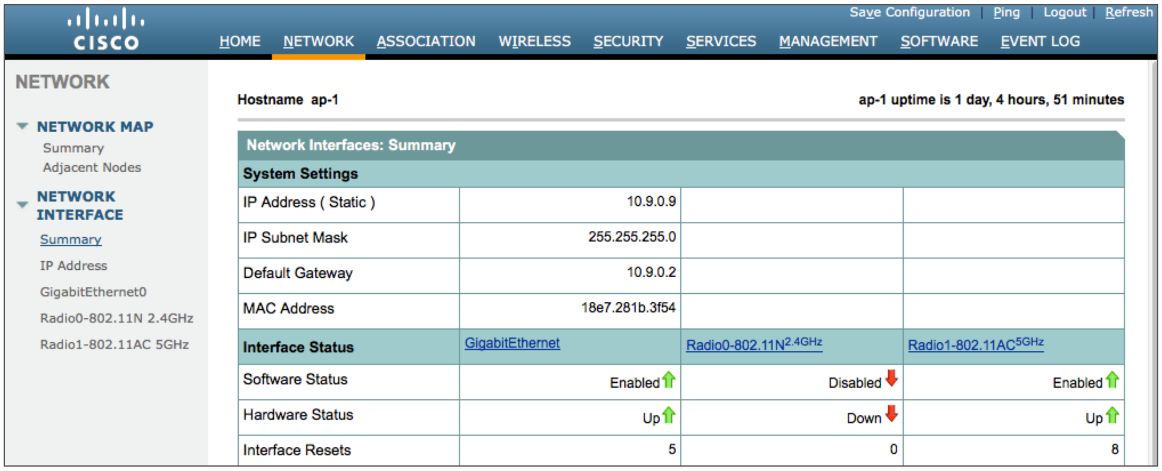
When configuring Cisco Autonomous Access Points, use the following guidelines:

- Configure the **Data Rates** as necessary
- Configure **Quality of Service (QoS)**
- Set the **WMM Policy** to **Required**
- Ensure **Aironet Extensions** is **Enabled**
- Disable **Public Secure Packet Forwarding (PSPF)**
- Set **IGMP Snooping** to **Enabled**

802.11 Network Settings

We recommend that you have the phone operate on the 5 GHz band only due to that there are many channels available on this band and not as many interferers as the 2.4 GHz band has.

To use the 5 GHz band, ensure that the 802.11a/n network status is **Enabled**.



Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 51 minutes

Network Interfaces: Summary

System Settings			
IP Address (Static)	10.9.0.9		
IP Subnet Mask	255.255.255.0		
Default Gateway	10.9.0.2		
MAC Address	18e7.281b.3f54		
Interface Status	GigabitEthernet	Radio0-802.11N$^{2.4GHz}$	Radio1-802.11AC^{5GHz}
Software Status	Enabled ↑	Disabled ↓	Enabled ↑
Hardware Status	Up ↑	Down ↓	Up ↑
Interface Resets	5	0	8

We recommend that you set 12 Mbps as the mandatory (basic) rate and 18 Mbps or higher as the supported (optional) rates. However, some environments may require 6 Mbps to be enabled as the mandatory (basic) rate.

When using the 5 GHz band, up to 12 channels only is recommended to avoid any potential delay of access point discovery due to having to scan many channels.

For Cisco Autonomous Access Points, select Dynamic Frequency Selection (DFS) to use auto channel selection.

When DFS is enabled, enable at least one band (bands 1-4).

You can select Band 1 only for the access point to use a UNII-1 channel (channel 36, 40, 44, or 48).

Individual access points can be configured to override the global settings to use dynamic channel and transmit power assignment for either 5 GHz or 2.4 GHz depending on the frequency band to be used.

Other access points can be enabled for Auto RF and workaround the access points that are statically configured.

This may be necessary if there is an intermittent interference present in an area.

The 5 GHz channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points and 20 MHz, 40 MHz, or 80 MHz if using Cisco 802.11ac Access Points.

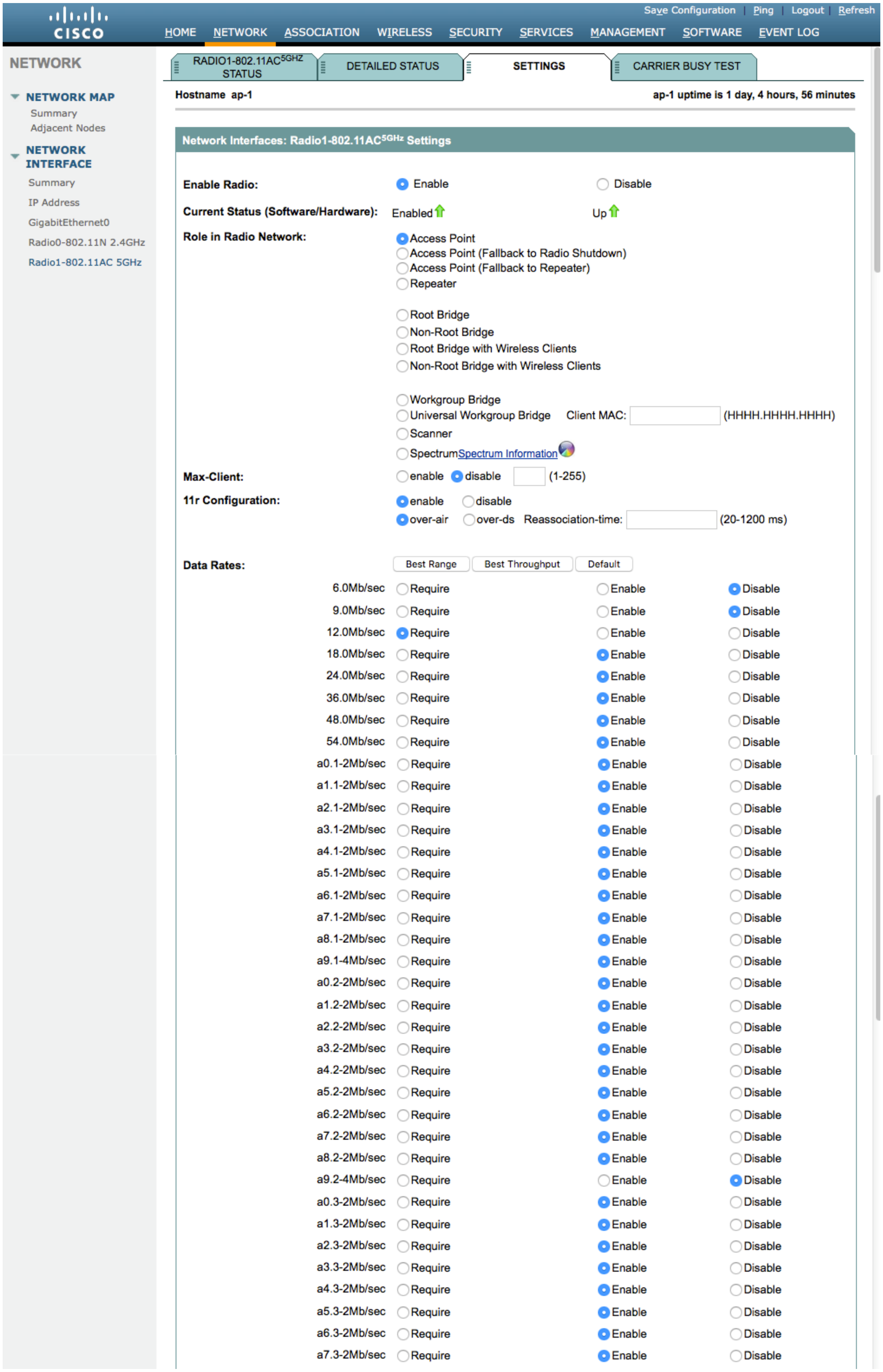
It is recommended to use the same channel width for all access points.

Ensure **Client Power** is configured properly. Do not use the default setting of **Max** power for client power on Cisco Autonomous Access Points because that will not advertise DTPC to the client.

Enable **Dot11d** for **World Mode** and configure the proper **Country Code**.

Ensure **Aironet Extensions** is enabled.

Set the **Beacon Period** to **100 ms** and **DTIM** to 2.



Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 56 minutes

Network Interfaces: Radio1-802.11AC5GHz Settings

Enable Radio:	● Enable	○ Disable
Current Status (Software/Hardware):	Enabled	Up

Role in Radio Network:

● Access Point
○ Access Point (Fallback to Radio Shutdown)
○ Access Point (Fallback to Repeater)
○ Repeater

○ Root Bridge
○ Non-Root Bridge
○ Root Bridge with Wireless Clients
○ Non-Root Bridge with Wireless Clients

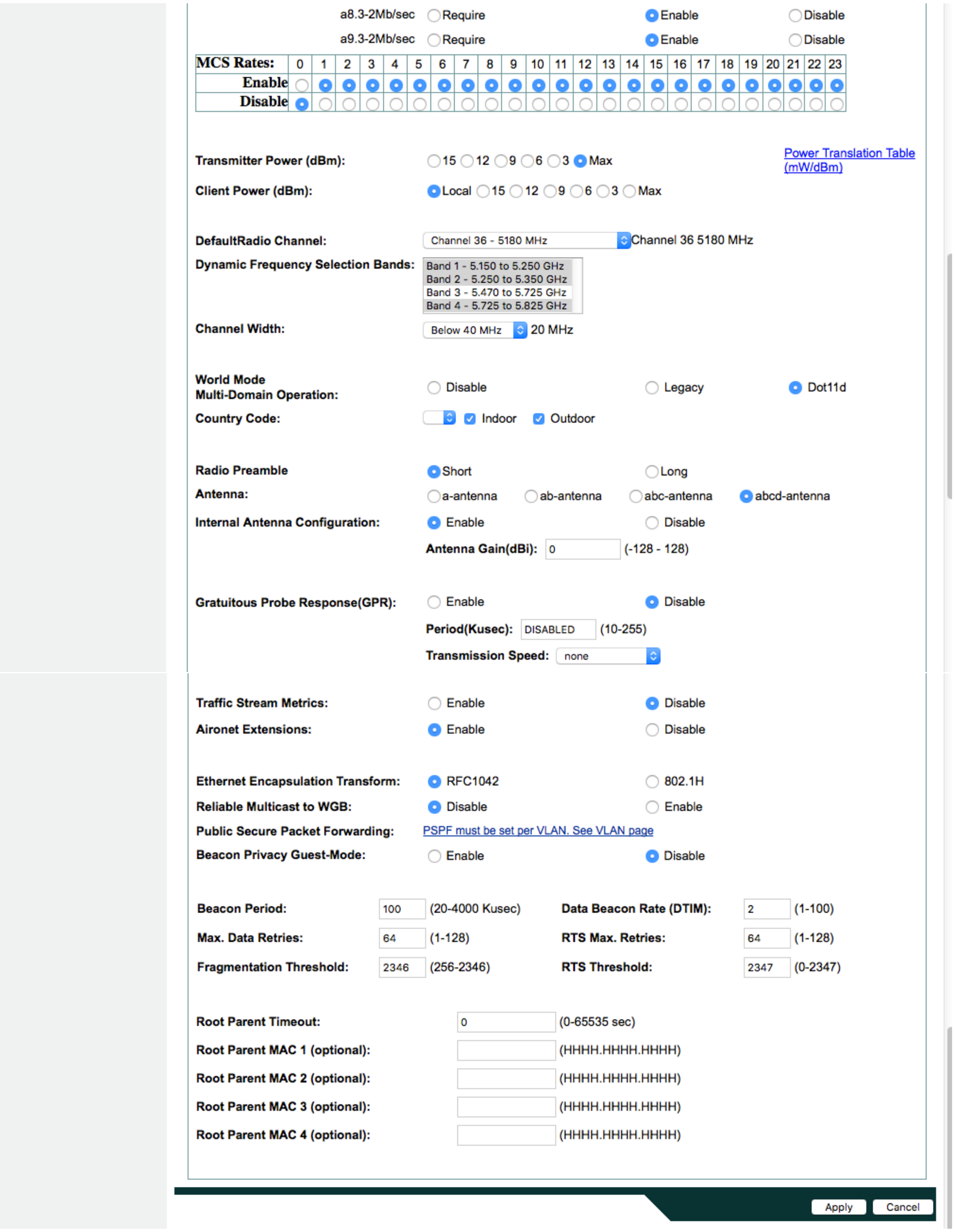
○ Workgroup Bridge
○ Universal Workgroup Bridge Client MAC: (HHHH.HHHH.HHHH)
○ Scanner
○ Spectrum Spectrum Information

Max-Client: ○ enable ● disable (1-255)

11r Configuration: ● enable ○ disable
● over-air ○ over-ds Reassociation-time: (20-1200 ms)

Data Rates: Best Range | Best Throughput | Default

6.0Mb/sec	○ Require	○ Enable	● Disable
9.0Mb/sec	○ Require	○ Enable	● Disable
12.0Mb/sec	● Require	○ Enable	○ Disable
18.0Mb/sec	○ Require	● Enable	○ Disable
24.0Mb/sec	○ Require	● Enable	○ Disable
36.0Mb/sec	○ Require	● Enable	○ Disable
48.0Mb/sec	○ Require	● Enable	○ Disable
54.0Mb/sec	○ Require	● Enable	○ Disable
a0.1-2Mb/sec	○ Require	● Enable	○ Disable
a1.1-2Mb/sec	○ Require	● Enable	○ Disable
a2.1-2Mb/sec	○ Require	● Enable	○ Disable
a3.1-2Mb/sec	○ Require	● Enable	○ Disable
a4.1-2Mb/sec	○ Require	● Enable	○ Disable
a5.1-2Mb/sec	○ Require	● Enable	○ Disable
a6.1-2Mb/sec	○ Require	● Enable	○ Disable
a7.1-2Mb/sec	○ Require	● Enable	○ Disable
a8.1-2Mb/sec	○ Require	● Enable	○ Disable
a9.1-4Mb/sec	○ Require	● Enable	○ Disable
a0.2-2Mb/sec	○ Require	● Enable	○ Disable
a1.2-2Mb/sec	○ Require	● Enable	○ Disable
a2.2-2Mb/sec	○ Require	● Enable	○ Disable
a3.2-2Mb/sec	○ Require	● Enable	○ Disable
a4.2-2Mb/sec	○ Require	● Enable	○ Disable
a5.2-2Mb/sec	○ Require	● Enable	○ Disable
a6.2-2Mb/sec	○ Require	● Enable	○ Disable
a7.2-2Mb/sec	○ Require	● Enable	○ Disable
a8.2-2Mb/sec	○ Require	● Enable	○ Disable
a9.2-4Mb/sec	○ Require	○ Enable	● Disable
a0.3-2Mb/sec	○ Require	● Enable	○ Disable
a1.3-2Mb/sec	○ Require	● Enable	○ Disable
a2.3-2Mb/sec	○ Require	● Enable	○ Disable
a3.3-2Mb/sec	○ Require	● Enable	○ Disable
a4.3-2Mb/sec	○ Require	● Enable	○ Disable
a5.3-2Mb/sec	○ Require	● Enable	○ Disable
a6.3-2Mb/sec	○ Require	● Enable	○ Disable
a7.3-2Mb/sec	○ Require	● Enable	○ Disable



a8.3-2Mb/sec ○ Require ● Enable ○ Disable

a9.3-2Mb/sec ○ Require ● Enable ○ Disable

MCS Rates:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Enable	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Transmitter Power (dBm): ○ 15 ○ 12 ○ 9 ○ 6 ○ 3 ● Max — Power Translation Table (mW/dBm)

Client Power (dBm): ● Local ○ 15 ○ 12 ○ 9 ○ 6 ○ 3 ○ Max

DefaultRadio Channel: Channel 36 - 5180 MHz Channel 36 5180 MHz

Dynamic Frequency Selection Bands:
Band 1 - 5.150 to 5.250 GHz
Band 2 - 5.250 to 5.350 GHz
Band 3 - 5.470 to 5.725 GHz
Band 4 - 5.725 to 5.825 GHz

Channel Width: Below 40 MHz 20 MHz

World Mode Multi-Domain Operation: ○ Disable ○ Legacy ● Dot11d

Country Code: ☑ Indoor ☑ Outdoor

Radio Preamble ● Short ○ Long

Antenna: ○ a-antenna ○ ab-antenna ○ abc-antenna ● abcd-antenna

Internal Antenna Configuration: ● Enable ○ Disable

Antenna Gain(dBi): 0 (-128 - 128)

Gratuitous Probe Response(GPR): ○ Enable ● Disable

Period(Kusec): DISABLED (10-255)

Transmission Speed: none

Traffic Stream Metrics: ○ Enable ● Disable

Aironet Extensions: ● Enable ○ Disable

Ethernet Encapsulation Transform: ● RFC1042 ○ 802.1H

Reliable Multicast to WGB: ● Disable ○ Enable

Public Secure Packet Forwarding: PSPF must be set per VLAN. See VLAN page

Beacon Privacy Guest-Mode: ○ Enable ● Disable

Beacon Period: 100 (20-4000 Kusec) **Data Beacon Rate (DTIM):** 2 (1-100)

Max. Data Retries: 64 (1-128) **RTS Max. Retries:** 64 (1-128)

Fragmentation Threshold: 2346 (256-2346) **RTS Threshold:** 2347 (0-2347)

Root Parent Timeout: 0 (0-65535 sec)

Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

If you want to use the 2.4 GHz band, ensure that the 802.11b/g/n network status and 802.11g is enabled.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18 Mbps or higher as supported (optional) rates assuming that there will not be any 802.11b-only clients connecting to the wireless LAN. However, some environments may require 6 Mbps to be enabled as the mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12 Mbps or higher as the supported (optional) rate.

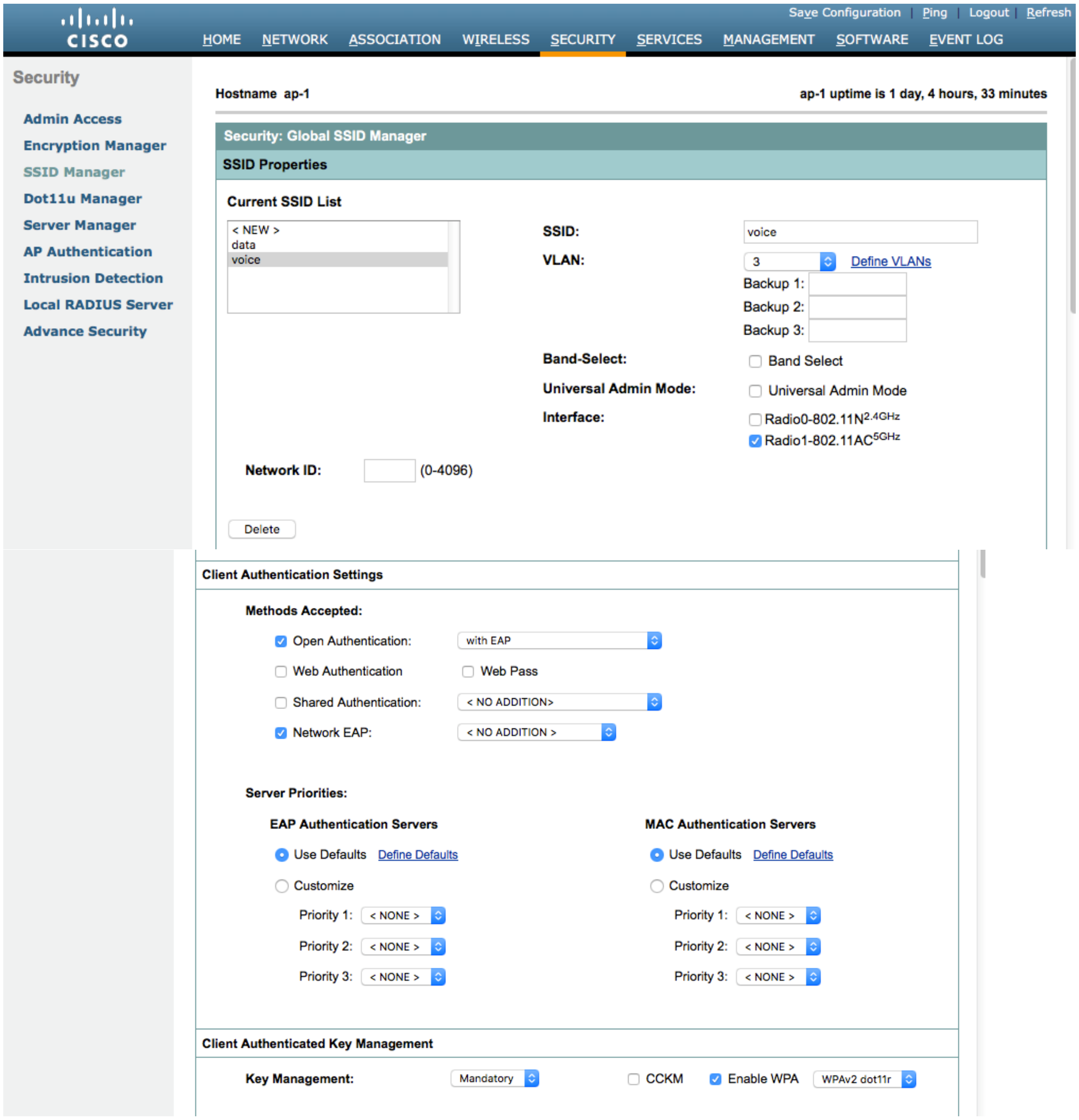
WLAN Settings

We recommend that you set a separate SSID for the phone to connect.

However, if there is an existing SSID configured to support voice-capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by the phone can be configured to only apply to a certain 802.11 radio type (e.g. 802.11a only).

Enable **WPA2** key management.



Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 33 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
data
voice

SSID: voice

VLAN: 3

Backup 1:

Backup 2:

Backup 3:

Band-Select: □ Band Select

Universal Admin Mode: □ Universal Admin Mode

Interface: □ Radio0-802.11N$^{2.4GHz}$
☑ Radio1-802.11AC^{5GHz}

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

□ Web Authentication □ Web Pass

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

● Use Defaults

○ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

● Use Defaults

○ Customize

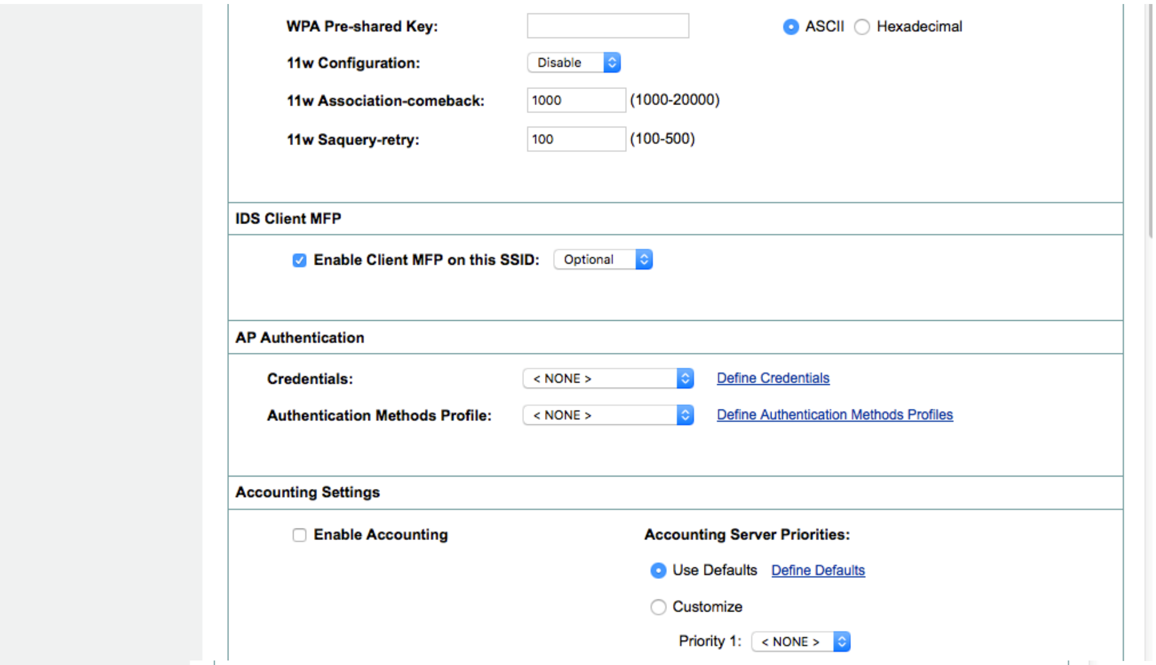
Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Client Authenticated Key Management

Key Management: Mandatory □ CCKM ☑ Enable WPA WPAv2 dot11r



WPA Pre-shared Key: ______ ● ASCII ○ Hexadecimal

11w Configuration: Disable

11w Association-comeback: 1000 (1000-20000)

11w Saquery-retry: 100 (100-500)

IDS Client MFP

☑ **Enable Client MFP on this SSID:** Optional

AP Authentication

Credentials: < NONE > Define Credentials

Authentication Methods Profile: < NONE > Define Authentication Methods Profiles

Accounting Settings

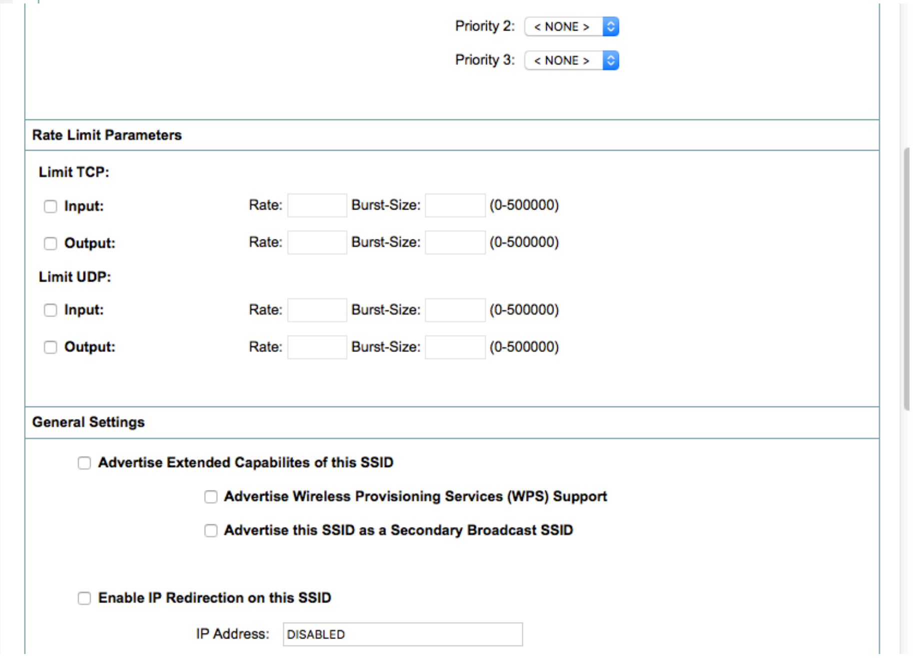
□ **Enable Accounting**

Accounting Server Priorities:

● Use Defaults Define Defaults

○ Customize

Priority 1: < NONE >



Priority 2: < NONE >

Priority 3: < NONE >

Rate Limit Parameters

Limit TCP:

□ **Input:** Rate: ______ Burst-Size: ______ (0-500000)

□ **Output:** Rate: ______ Burst-Size: ______ (0-500000)

Limit UDP:

□ **Input:** Rate: ______ Burst-Size: ______ (0-500000)

□ **Output:** Rate: ______ Burst-Size: ______ (0-500000)

General Settings

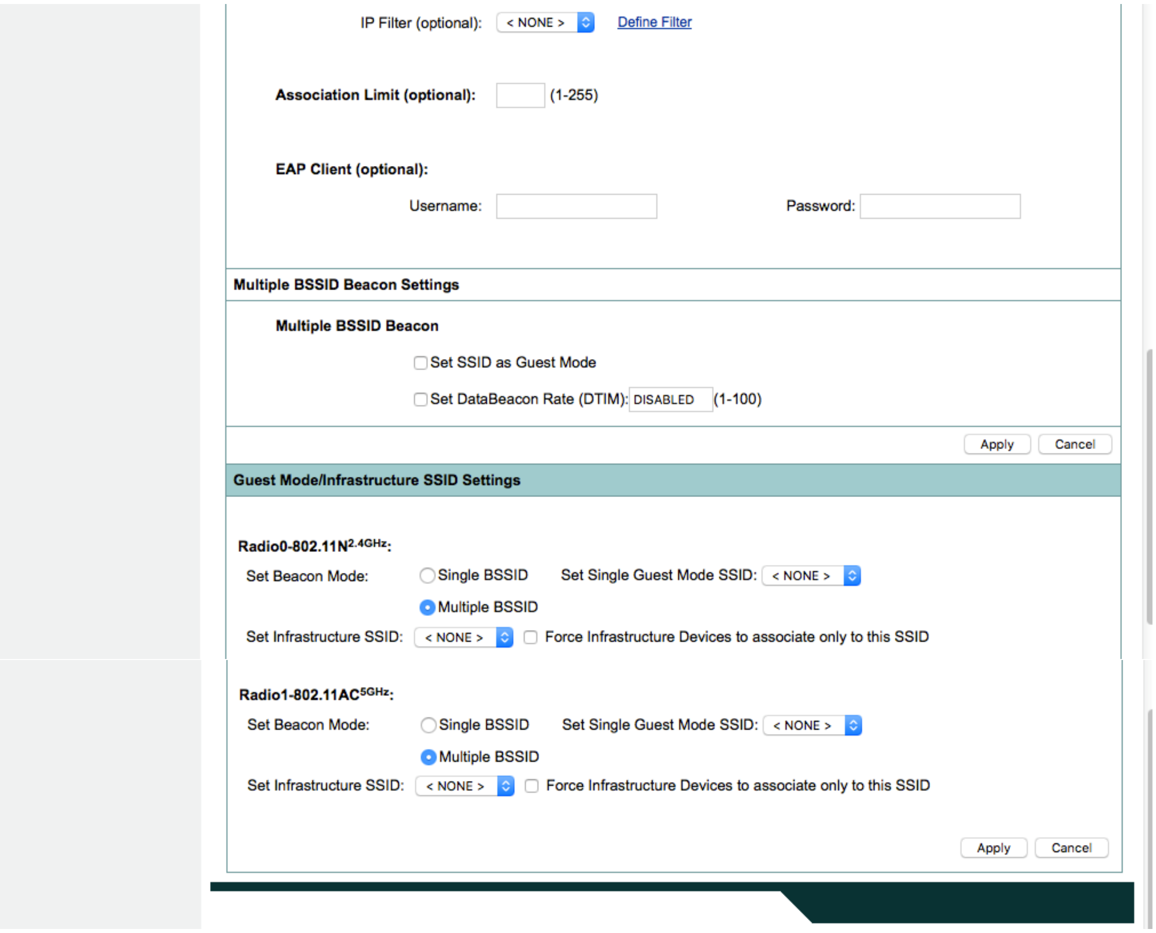
□ **Advertise Extended Capabilites of this SSID**

□ **Advertise Wireless Provisioning Services (WPS) Support**

□ **Advertise this SSID as a Secondary Broadcast SSID**

□ **Enable IP Redirection on this SSID**

IP Address: DISABLED



IP Filter (optional): < NONE > Define Filter

Association Limit (optional): (1-255)

EAP Client (optional):

Username: Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

□ Set SSID as Guest Mode

□ Set DataBeacon Rate (DTIM): DISABLED (1-100)

Guest Mode/Infrastructure SSID Settings

Radio0-802.11N$^{2.4GHz}$:

Set Beacon Mode: ○ Single BSSID Set Single Guest Mode SSID: < NONE >

● Multiple BSSID

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

Radio1-802.11AC^{5GHz}:

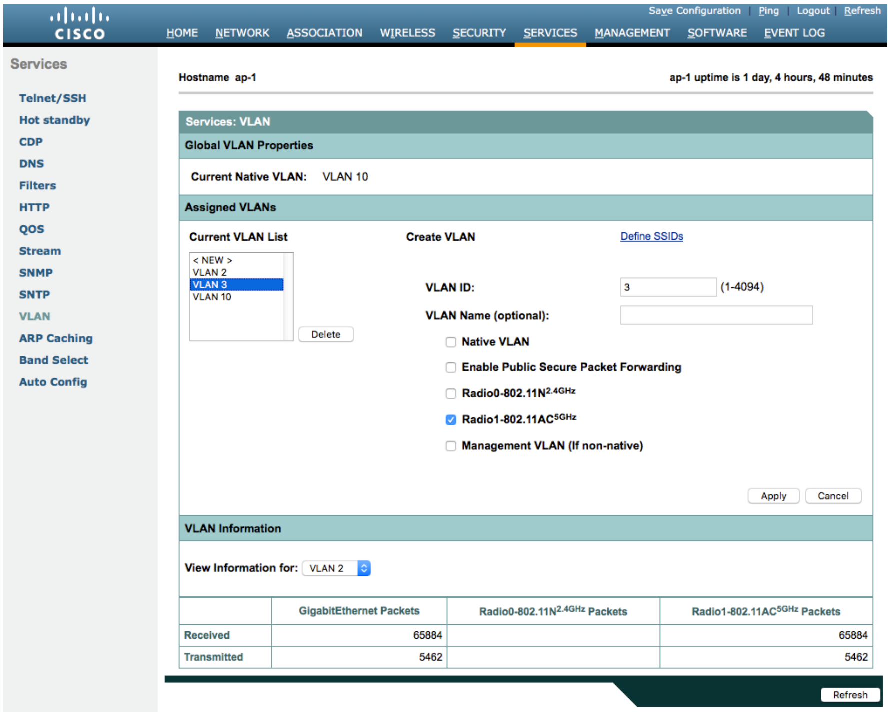
Set Beacon Mode: ○ Single BSSID Set Single Guest Mode SSID: < NONE >

● Multiple BSSID

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

Segment wireless voice and data into separate VLANs.

Ensure that Public Secure Packet Forwarding (PSPF) is not enabled for the voice VLAN as this will prevent clients from direct communication when associated to the same access point. If PSPF is enabled, then the result will be no audio.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Services
Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config
Delete
Apply
Cancel
Refresh

Hostname ap-1 — ap-1 uptime is 1 day, 4 hours, 48 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 10

Assigned VLANs

Current VLAN List: < NEW >, VLAN 2, VLAN 3 (selected), VLAN 10

Create VLAN — Define SSIDs

VLAN ID: 3 (1-4094)

VLAN Name (optional):

☐ Native VLAN

☐ Enable Public Secure Packet Forwarding

☐ Radio0-802.11N 2.4GHz

☑ Radio1-802.11AC 5GHz

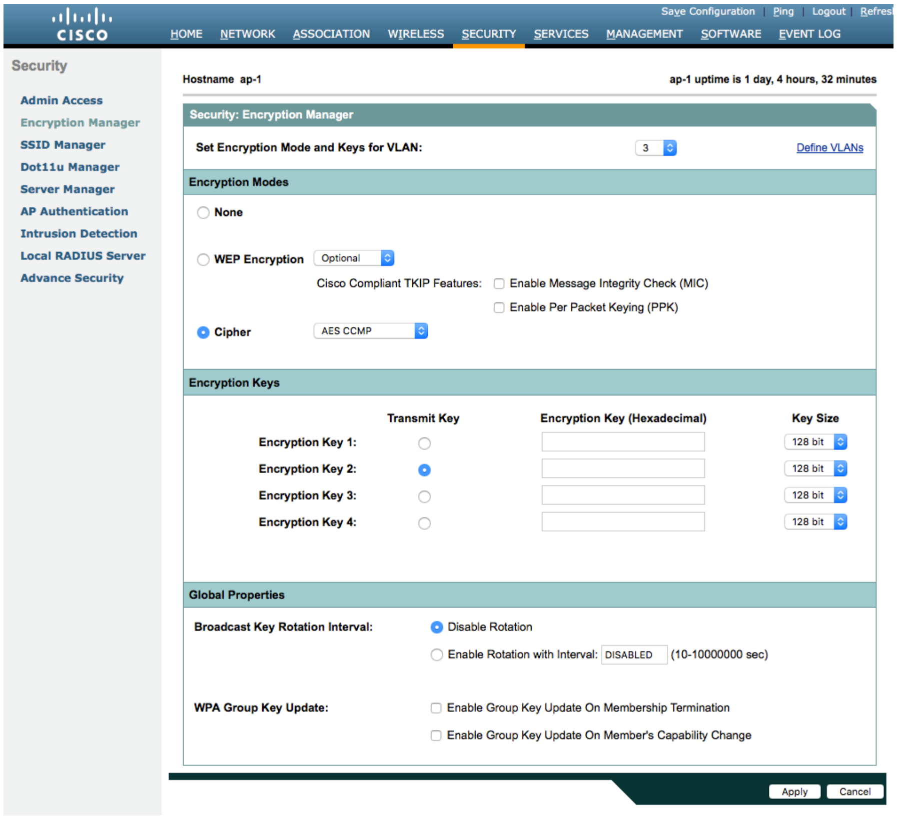
☐ Management VLAN (If non-native)

VLAN Information

View Information for: VLAN 2

	GigabitEthernet Packets	Radio0-802.11N 2.4GHz Packets	Radio1-802.11AC 5GHz Packets
Received	65884		65884
Transmitted	5462		5462

Ensure **AES** is selected for encryption type.



Hostname ap-1 — ap-1 uptime is 1 day, 4 hours, 32 minutes

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3 — Define VLANs

Encryption Modes

○ None

○ WEP Encryption: Optional

Cisco Compliant TKIP Features: ☐ Enable Message Integrity Check (MIC) ☐ Enable Per Packet Keying (PPK)

● Cipher: AES CCMP

Encryption Keys

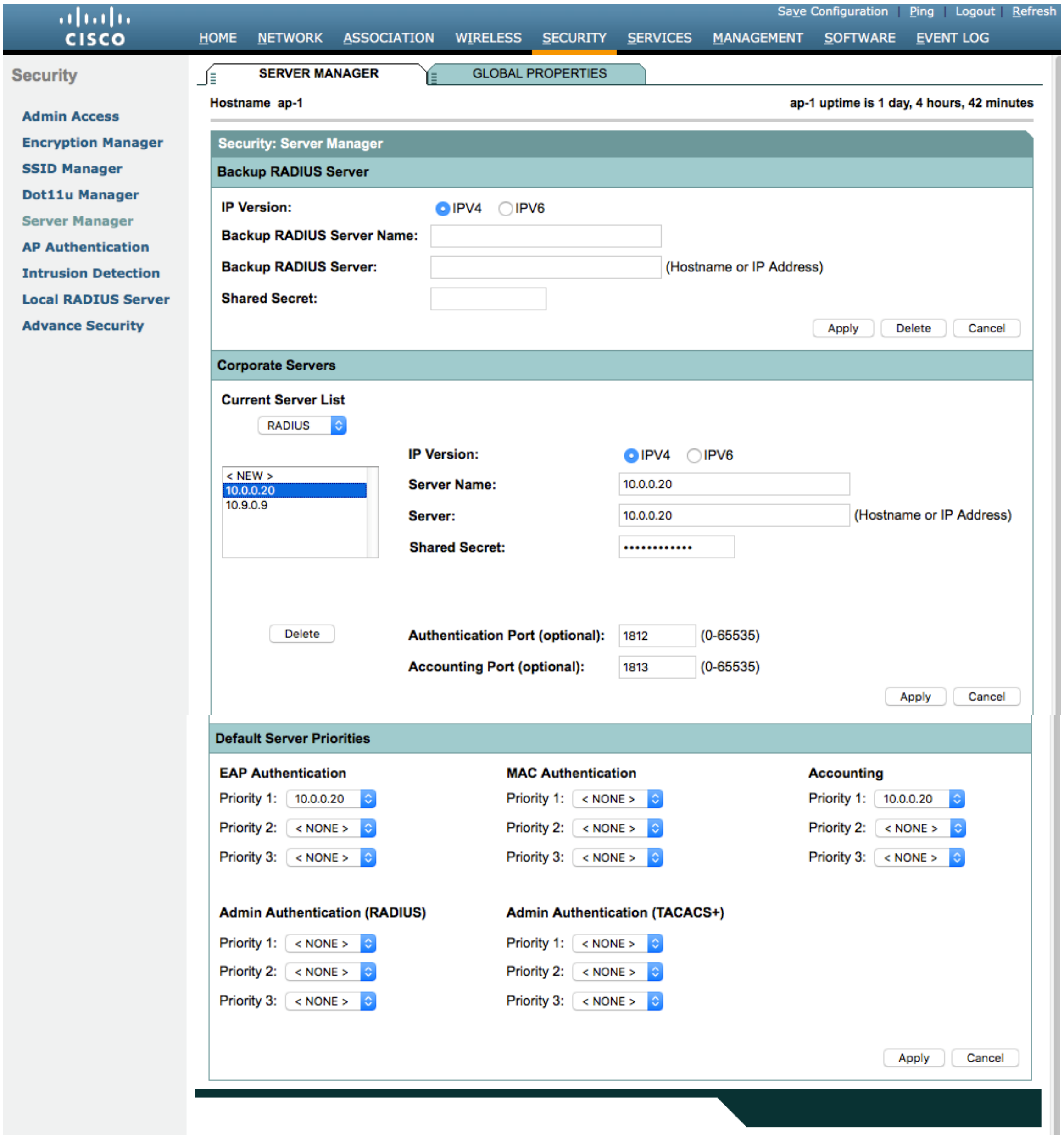
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Global Properties

Broadcast Key Rotation Interval: ● Disable Rotation ○ Enable Rotation with Interval: DISABLED (10-10000000 sec)

WPA Group Key Update: ☐ Enable Group Key Update On Membership Termination ☐ Enable Group Key Update On Member's Capability Change

Configure the RADIUS servers to be used for authentication and accounting.



Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 42 minutes

Security: Server Manager

Backup RADIUS Server

IP Version: ● IPV4 ○ IPV6

Backup RADIUS Server Name:

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Corporate Servers

Current Server List

RADIUS

< NEW >
10.0.0.20
10.9.0.9

IP Version: ● IPV4 ○ IPV6

Server Name: 10.0.0.20

Server: 10.0.0.20 (Hostname or IP Address)

Shared Secret: ••••••••••••

Authentication Port (optional): 1812 (0-65535)

Accounting Port (optional): 1813 (0-65535)

Default Server Priorities

EAP Authentication		MAC Authentication		Accounting	
Priority 1:	10.0.0.20	Priority 1:	< NONE >	Priority 1:	10.0.0.20
Priority 2:	< NONE >	Priority 2:	< NONE >	Priority 2:	< NONE >
Priority 3:	< NONE >	Priority 3:	< NONE >	Priority 3:	< NONE >

Admin Authentication (RADIUS)		Admin Authentication (TACACS+)	
Priority 1:	< NONE >	Priority 1:	< NONE >
Priority 2:	< NONE >	Priority 2:	< NONE >
Priority 3:	< NONE >	Priority 3:	< NONE >

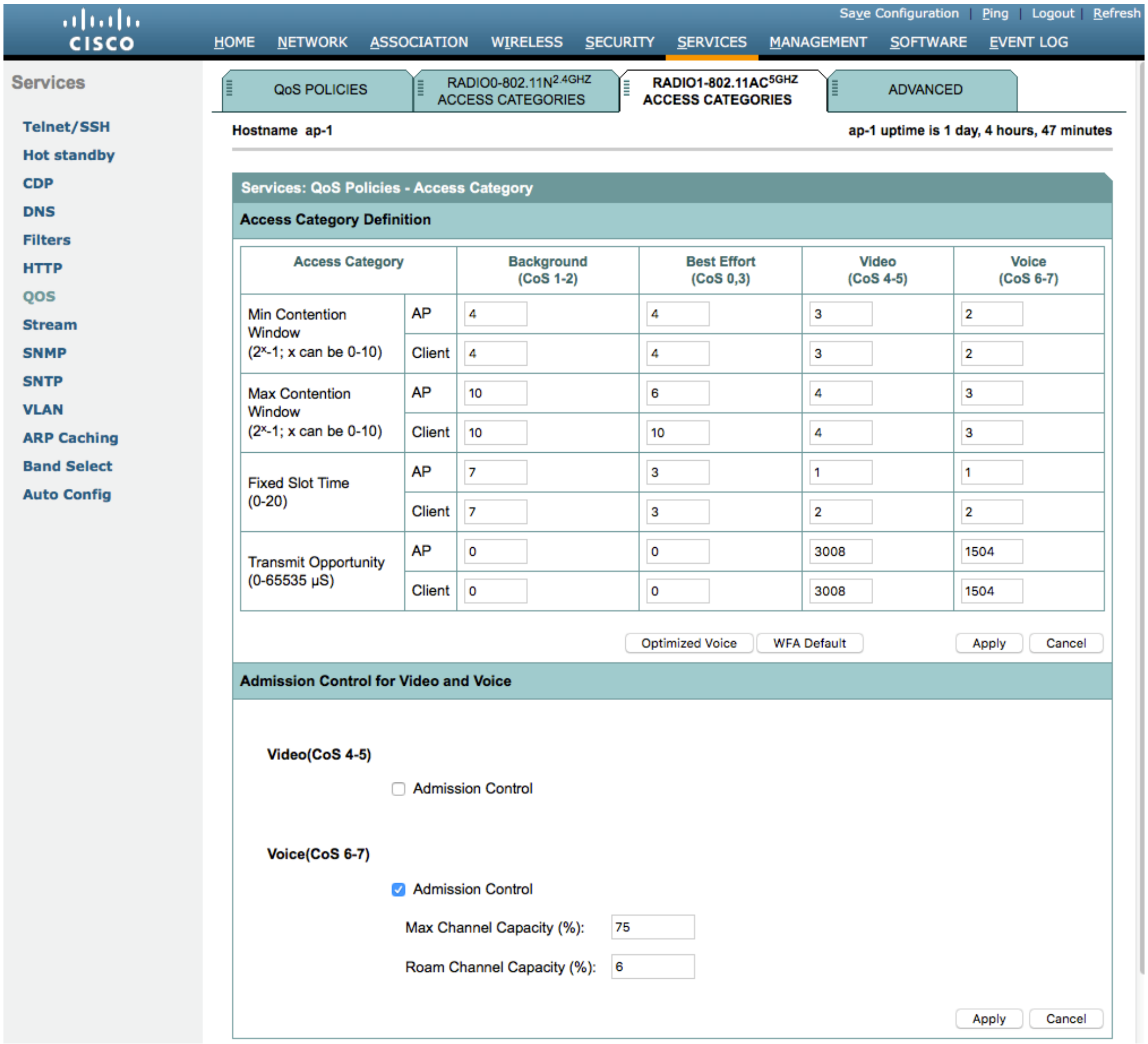
Call Admission Control (CAC)

Load-based CAC that supports multiple streams is not present on the Cisco Autonomous Access Points therefore it is not recommended to enable CAC on Cisco Autonomous Access points.

The Cisco Autonomous Access Point only allows for one stream and the stream size is not customizable, therefore SRTP and barge do not work if CAC is enabled.

If Admission Control for Voice or for Video is enabled on the Cisco Autonomous Access Point, the admission must be unblocked on the SSID as well. In recent releases, the admission is unblocked by default.

```
dot11 ssid voice
   vlan 3
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2 dot11r
   admit-traffic
```


cisco
Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Services
Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config
QoS POLICIES
RADIO0-802.11N 2.4GHZ ACCESS CATEGORIES
RADIO1-802.11AC 5GHZ ACCESS CATEGORIES
ADVANCED

Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 47 minutes

Services: QoS Policies - Access Category

Access Category Definition

Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2^x-1; x can be 0-10)	AP	4	4	3	2
	Client	4	4	3	2
Max Contention Window (2^x-1; x can be 0-10)	AP	10	6	4	3
	Client	10	10	4	3
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 µS)	AP	0	0	3008	1504
	Client	0	0	3008	1504

Admission Control for Video and Voice

Video(CoS 4-5)

□ Admission Control

Voice(CoS 6-7)

☑ Admission Control

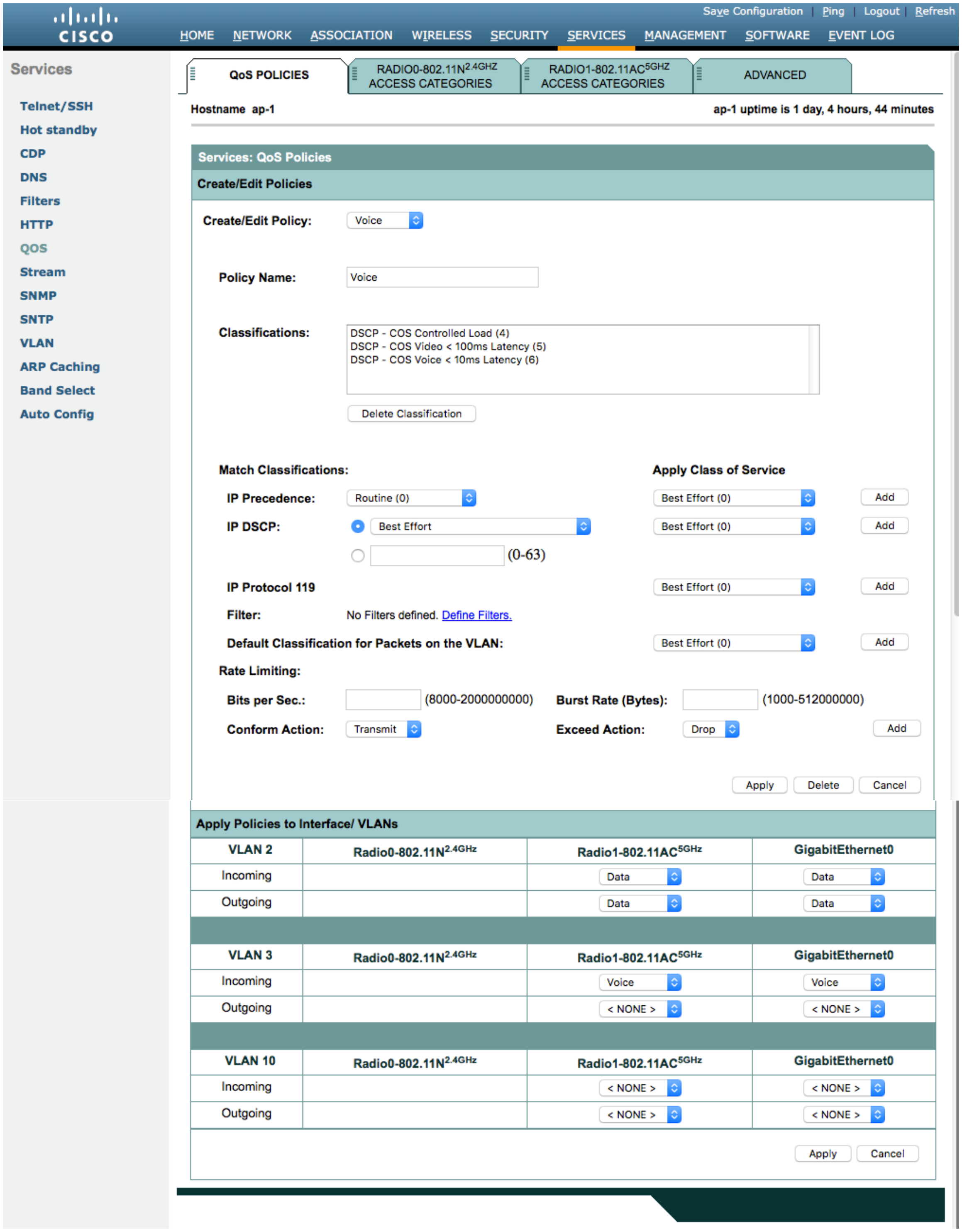
Max Channel Capacity (%): 75

Roam Channel Capacity (%): 6

QoS Policies

Configure the following QoS policy on the Cisco Autonomous Access Point to enable DSCP to CoS (WMM UP) mapping.

This allows packets to be placed into the proper queue as long as those packets are marked correctly when received at the access point level.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Services
Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config
QoS POLICIES
RADIO0-802.11N2.4GHZ ACCESS CATEGORIES
RADIO1-802.11AC5GHZ ACCESS CATEGORIES
ADVANCED

Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 44 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: Voice

Policy Name: Voice

Classifications:
DSCP - COS Controlled Load (4)
DSCP - COS Video < 100ms Latency (5)
DSCP - COS Voice < 10ms Latency (6)

Delete Classification

Match Classifications:		Apply Class of Service	
IP Precedence:	Routine (0)	Best Effort (0)	Add
IP DSCP:	● Best Effort	Best Effort (0)	Add
	○ (0-63)		
IP Protocol 119		Best Effort (0)	Add
Filter:	No Filters defined. Define Filters.		
Default Classification for Packets on the VLAN:		Best Effort (0)	Add

Rate Limiting:

Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000)

Conform Action: Transmit Exceed Action: Drop Add

Apply Delete Cancel

Apply Policies to Interface/ VLANs

VLAN 2	Radio0-802.11N$^{2.4GHz}$	Radio1-802.11AC^{5GHz}	GigabitEthernet0
Incoming		Data	Data
Outgoing		Data	Data
VLAN 3	**Radio0-802.11N$^{2.4GHz}$**	**Radio1-802.11AC^{5GHz}**	**GigabitEthernet0**
Incoming		Voice	Voice
Outgoing		< NONE >	< NONE >
VLAN 10	**Radio0-802.11N$^{2.4GHz}$**	**Radio1-802.11AC^{5GHz}**	**GigabitEthernet0**
Incoming		< NONE >	< NONE >
Outgoing		< NONE >	< NONE >

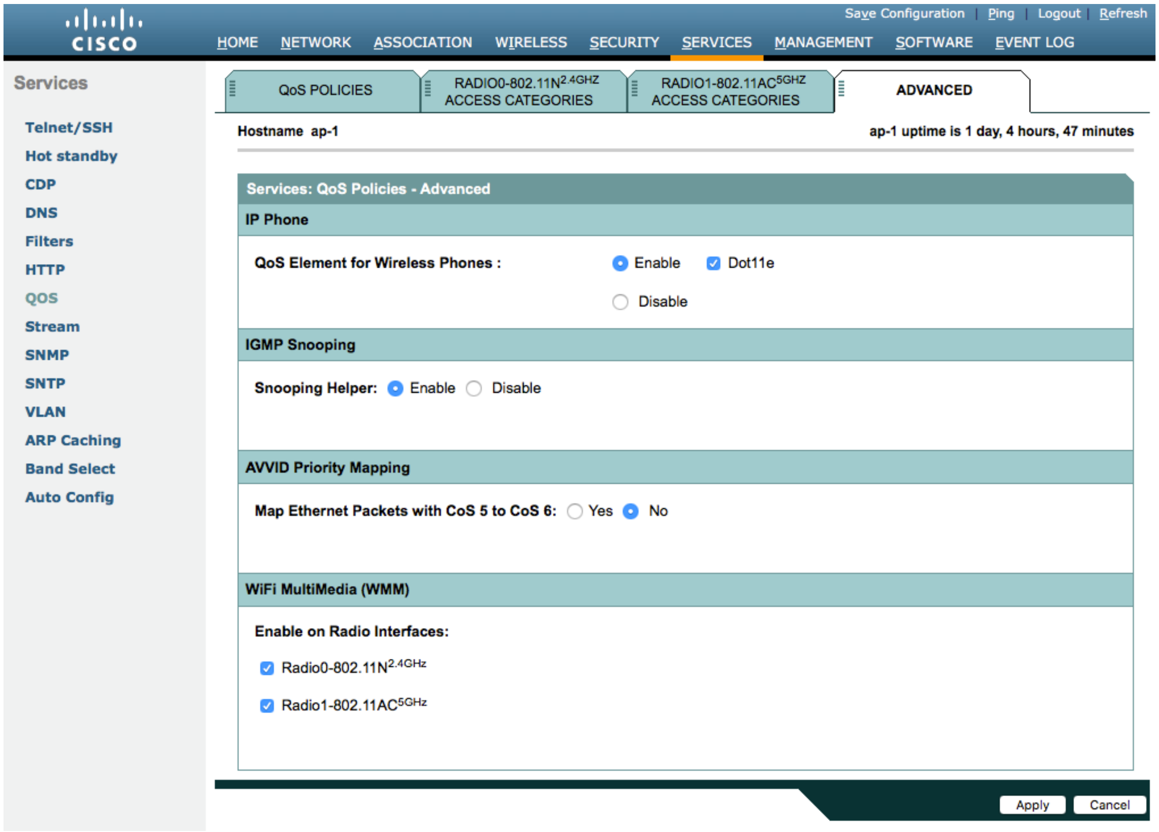
Apply Cancel

To enable QBSS, select **Enable** and check **Dot11e**.

If **Dot11e** is checked, then both CCA versions (802.11e and Cisco version 2) will be enabled.

Ensure **IGMP Snooping** is enabled.

Ensure **Wi-Fi MultiMedia (WMM)** is enabled.


Save Configuration | Ping | Logout | Refresh
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Services
Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Auto Config
QoS POLICIES
RADIO0-802.11N2.4GHZ ACCESS CATEGORIES
RADIO1-802.11AC5GHZ ACCESS CATEGORIES
ADVANCED
Apply
Cancel

Hostname ap-1 | ap-1 uptime is 1 day, 4 hours, 47 minutes

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones : ● Enable ☑ Dot11e ○ Disable

IGMP Snooping

Snooping Helper: ● Enable ○ Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6: ○ Yes ● No

WiFi MultiMedia (WMM)

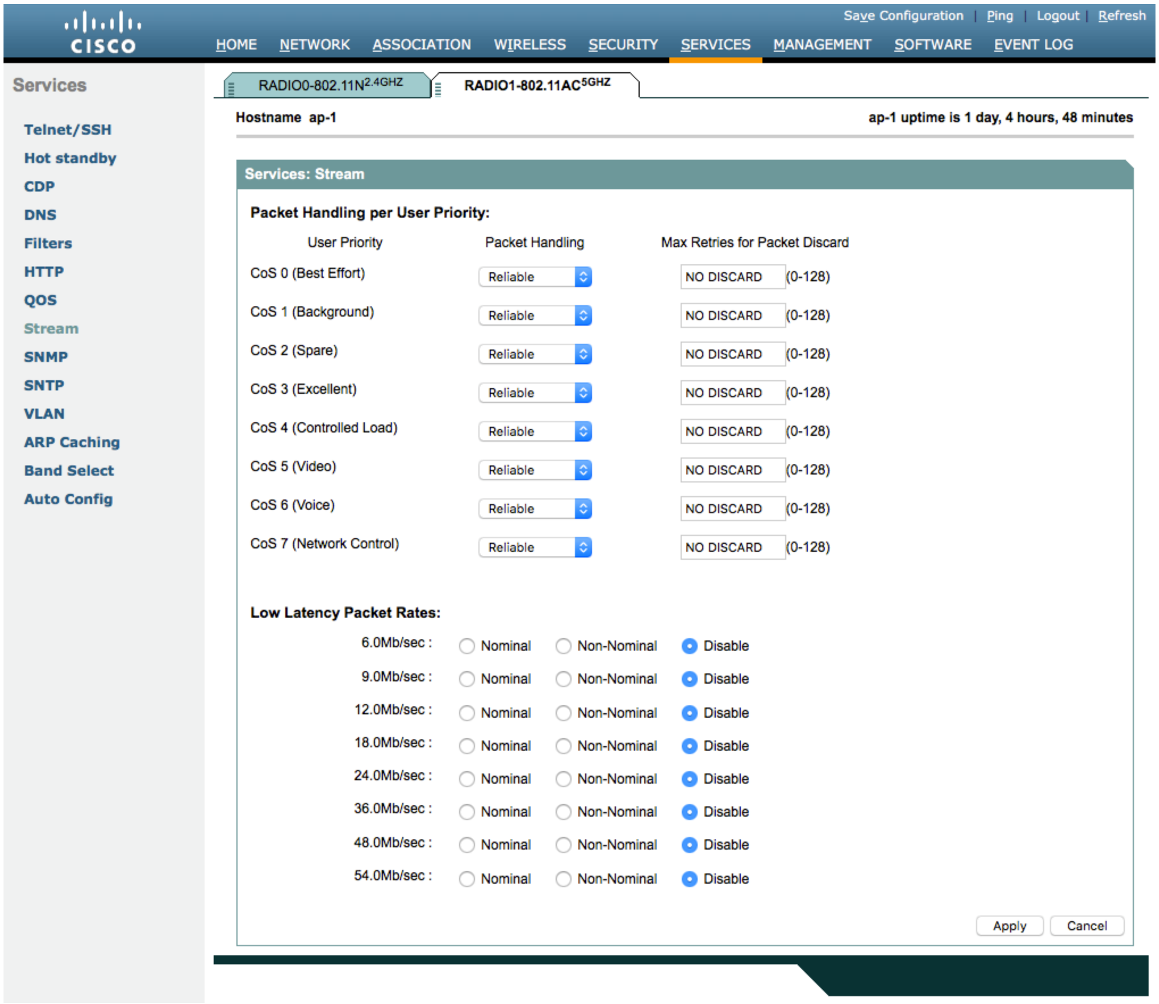
Enable on Radio Interfaces:

☑ Radio0-802.11N2.4GHz

☑ Radio1-802.11AC5GHz

If the **Stream** feature is enabled either directly or via selecting **Optimized Voice** for the radio access category in the QoS configuration section, then use the default settings, where 5.5, 6, 11, 12, and 24 Mbps are enabled as nominal rates for 802.11b/g, 6, 12, and 24 Mbps are enabled for 802.11a, and 6.5, 13, and 26 Mbps are enabled for 802.11n.

If the **Stream** feature is enabled, ensure that only voice packets are being put into the voice queue. Signaling packets (SIP) should be put into a separate queue. This can be ensured by setting up a QoS policy mapping the DSCP to the correct queue.



Hostname ap-1

ap-1 uptime is 1 day, 4 hours, 48 minutes

Services: Stream

Packet Handling per User Priority:

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Reliable	NO DISCARD (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

Low Latency Packet Rates:

6.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
9.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
12.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
18.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
24.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
36.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
48.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
54.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable

Advanced Settings

TKIP Countermeasure Holdoff Time

TKIP countermeasure mode can occur if the access point receives two Message Integrity Check (MIC) errors within 60 seconds. When this occurs, the access point will de-authenticate all TKIP clients associated to that 802.11 radio and hold off any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Autonomous Access Point, telnet or SSH to the access point and enter the following command specifying the number of seconds and WLAN ID.

```
Interface dot11radio X
countermeasure tkip hold-time <nseconds>
```

Configure Wireless Connection on Your Phone

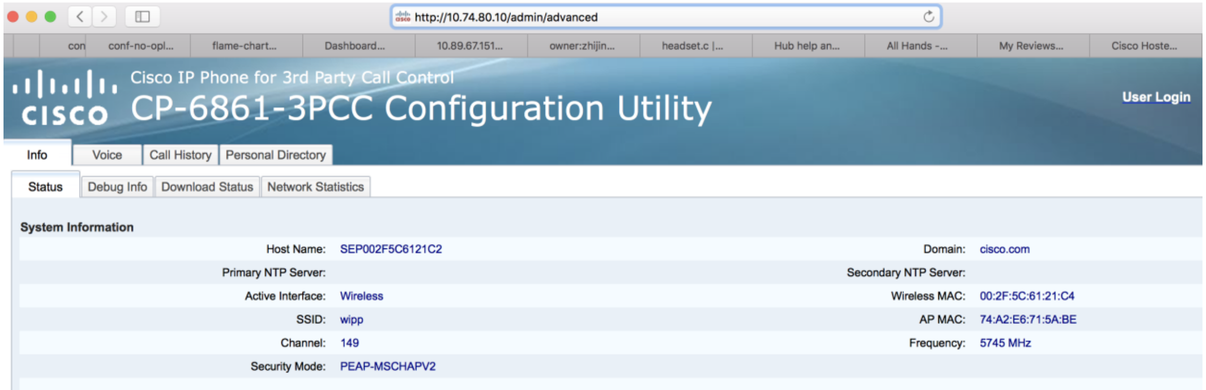
You can connect your phone to a wireless network through WLAN profiles or WPS. WLAN profiles can be configured on the phone web page, on the phone screen, or in the configuration file by remote provisioning.

Wireless LAN Profiles (Web Page)

Be sure that your phone has got a valid IP address either by wired or wireless connection, and you have the administrator access to your phone.

2. Access the phone administrator web page by visiting one of the following URL and enter the administrator password when prompted.

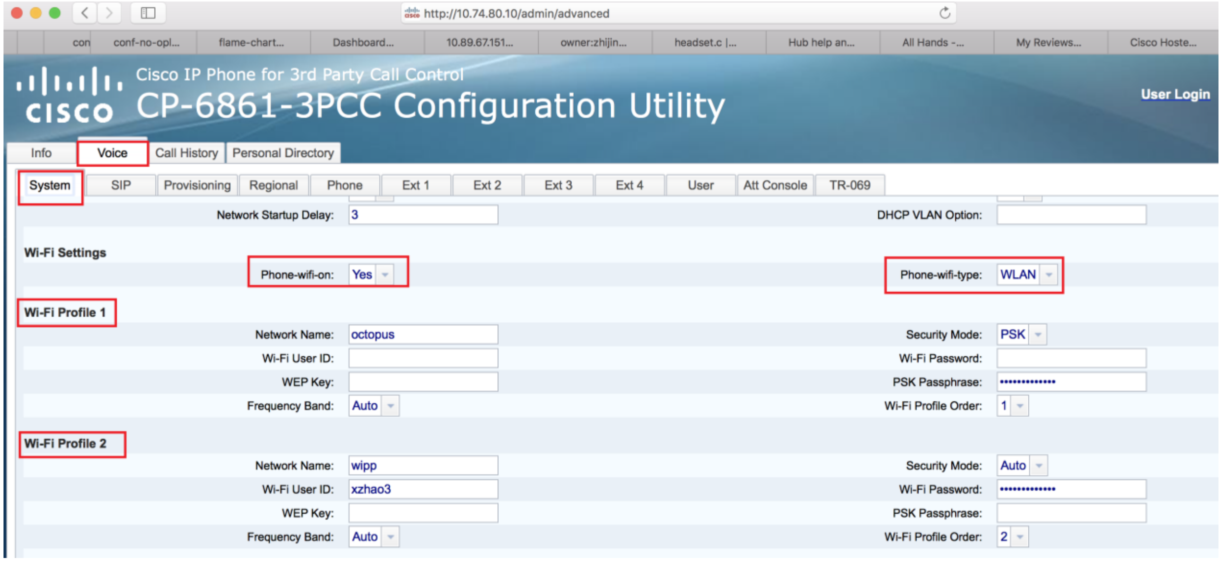
   http://<phone_IP>/admin/advanced, or https://<phone_IP>/admin/advanced



System Information

Host Name: SEP002F5C6121C2
Domain: cisco.com
Primary NTP Server:
Secondary NTP Server:
Active Interface: Wireless
Wireless MAC: 00:2F:5C:61:21:C4
SSID: wipp
AP MAC: 74:A2:E6:71:5A:BE
Channel: 149
Frequency: 5745 MHz
Security Mode: PEAP-MSCHAPV2

3. Go to the **Wi-Fi Settings** section on the **Voice > System** tab.



Network Startup Delay: 3
DHCP VLAN Option:

Wi-Fi Settings

Phone-wifi-on: Yes
Phone-wifi-type: WLAN

Wi-Fi Profile 1

Network Name: octopus
Security Mode: PSK
Wi-Fi User ID:
Wi-Fi Password:
WEP Key:
PSK Passphrase: •••••••••••••
Frequency Band: Auto
Wi-Fi Profile Order: 1

Wi-Fi Profile 2

Network Name: wipp
Security Mode: Auto
Wi-Fi User ID: xzhao3
Wi-Fi Password: •••••••••••••
WEP Key:
PSK Passphrase:
Frequency Band: Auto
Wi-Fi Profile Order: 2

The Cisco IP Phone 6861 Multiplatform Phone supports 4 Wi-Fi profiles. When you set **Phone-wifi-on** to **Yes** and **Phone-wifi-type** to **WLAN**, the phone tries the 4 profiles in the sequence defined in **Wi-Fi Profile Order** field. For each Wi-Fi profile, **Network Name** refers to the SSID of the AP you want to connect to.

Security Mode provides 7 options: **Auto**, **EAP-Fast**, **PEAP-GTC**, **PEAP-MSCHAPV2**, **PSK**, **WEP** and **NONE**. **Security Mode** selection is determined by the authentication method your target AP uses.

- If EAP-FAST, PEAP-MSCHAPv2, or PEAP-GTC is selected then Wi-Fi User ID and Wi-Fi Password are required.

- If PSK is selected to utilize Pre-Shared Key authentication, then a PSK Passphrase must be entered. The PSK Passphrase must be 8-63 ASCII character string.

- If WEP is selected to utilize static WEP (Wired Equivalent Privacy) authentication, then a WEP Key must be entered.

- Only WEP key 1 is supported. The entered key must match the transmit key on the access point side. The WEP Key must be in one of the following formats:

  - **40/64 Bit Key** = 5 digits ASCII or 10 digits HEX character string

  - **104/128 Bit Key** = 13 digits ASCII or 26 digits HEX character string

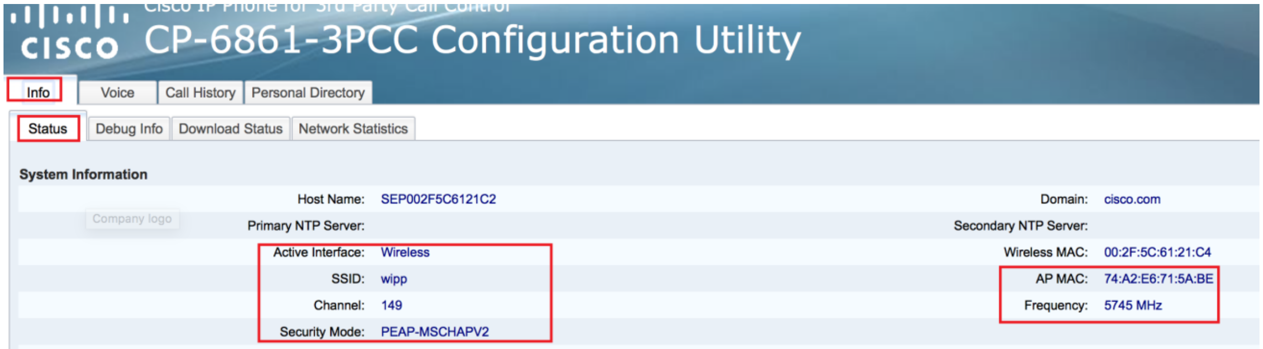
- If **None** is selected, then no authentication is required and no encryption will be utilized.

- If **Auto** is selected, your phone dynamically chooses **EAP-FAST**, **PEAP-MSCHAPv2**, or **PEAP-GTC** as authentication method based on communication with the target AP.

Frequency Band supports 5G, 2.4G, and Auto. Select the desired **Frequency Band** option:

- **Auto** = Gives preference to 5 GHz channels, but operates on both 5 GHz and 2.4 GHz channels
- **2.4 GHz** = Operates on 2.4 GHz channels only
- **5 GHz** = Operates on 5 GHz channels only

Once the phone connects to the target AP, the connection info would be displayed on phone's web portal as the following picture shows. Click the **Info** > **Status** to view the connection information.



System Information

Host Name: SEP002F5C6121C2
Domain: cisco.com
Primary NTP Server:
Secondary NTP Server:
Active Interface: Wireless
Wireless MAC: 00:2F:5C:61:21:C4
SSID: wipp
AP MAC: 74:A2:E6:71:5A:BE
Channel: 149
Frequency: 5745 MHz
Security Mode: PEAP-MSCHAPV2

Notes:

- Any change to the currently connected Wi-Fi profile would cause the phone to disconnect with the current AP, warm reboot, then connect to current AP with the changed parameters.

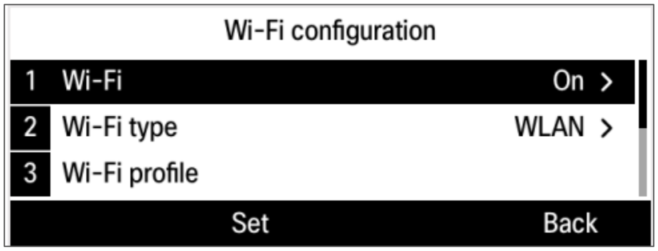
- If you have a wired network deployed on your site, connect your phone to the wired network first. After configuring Wi-Fi profiles on the phone web page, you can force the phone to connect to the configured profile by disconnecting the wired network.

- All the Wi-Fi profiles are saved on the phone. The phone can recover the previous Wi-Fi connection after a power cycle.

Wireless LAN Profiles (on Phone Screen)

To configure the Wi-Fi profiles on the phone screen, navigate to **Network configuration > Wi-Fi configuration > Wi-Fi profile**.

On the **Wi-Fi configuration** menu, choose **On** for **Wi-Fi** and **WLAN** for **Wi-Fi type**.



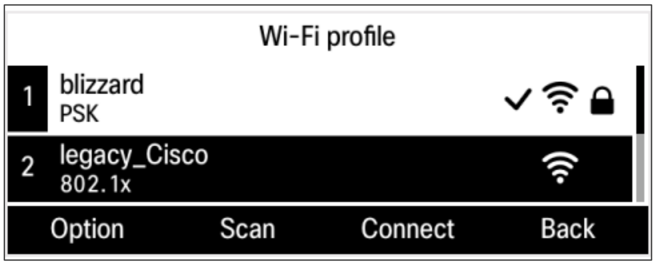
Wi-Fi configuration

1 Wi-Fi On >

2 Wi-Fi type WLAN >

3 Wi-Fi profile

The following picture shows the pre-saved profiles and the connected AP blizzard with PSK method.



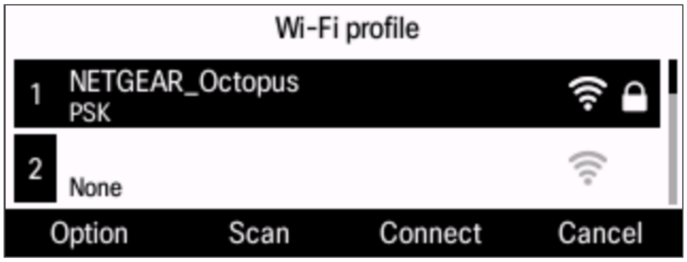
Wi-Fi profile

1 blizzard PSK ✓

2 legacy_Cisco 802.1x

- Create a new profile
  In the **Wi-Fi profile** page, select an empty profile and choose **Edit** from the **Option** menu. Enter all the necessary information in the **Edit profile** page and press **Save**.

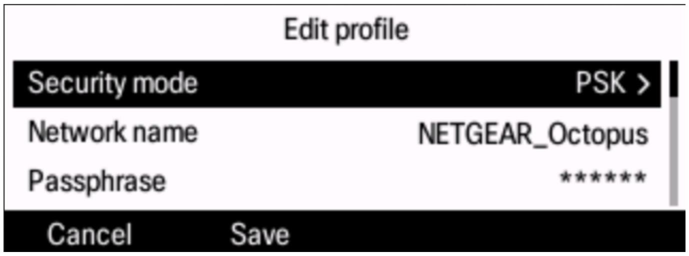
- Edit an existing profile
  In the **Wi-Fi profile** page, select an existing profile and choose **Edit** from the **Option** menu. Modify the settings in the **Edit profile** page and press **Save**.



Wi-Fi profile

1 NETGEAR_Octopus PSK

2 None



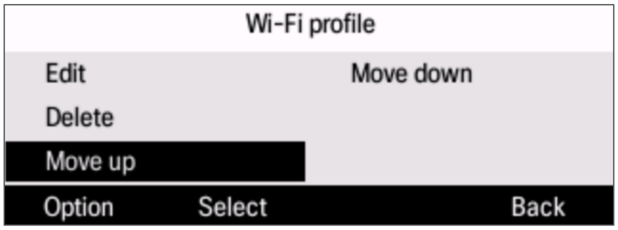
Edit profile

Security mode PSK >

Network name NETGEAR_Octopus

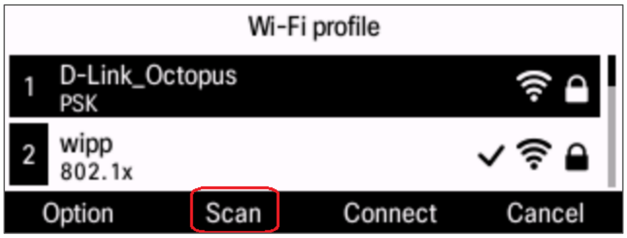
Passphrase ******

- Modify the order for a profile
  Your phone supports 4 Wi-Fi profiles. The phone continuously tries all the pre-saved profiles when Wi-Fi connection is lost until it connects with an AP. The trying order is from profile 1 to profile 4. To change the order of a profile, select the profile and chose **Move up** or **Move down** from the **Option** menu.

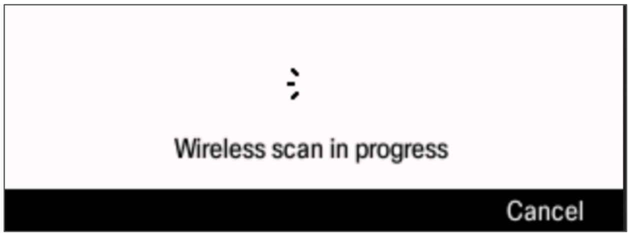


- Delete a profile
  To delete a profile, select the profile and choose **Delete** from the **Option** menu. Press **OK** to confirm.

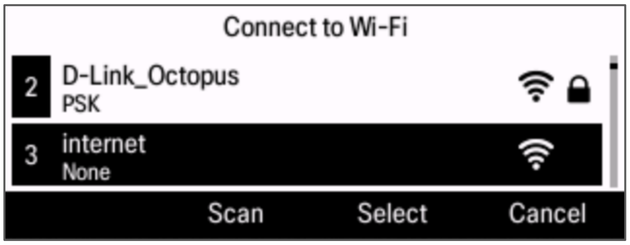
- Scan available AP
  In **Wi-Fi profile** page, choose **Scan** to search for the available access points. You can choose a wireless network from the scanned result to configure or connect to it.



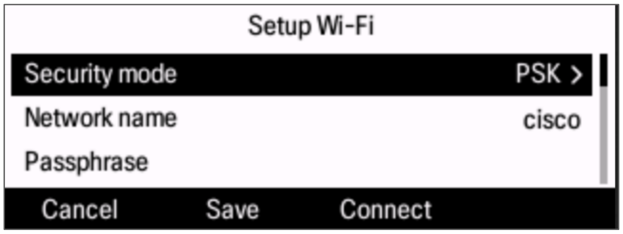
Once the **Scan** softkey is pressed, the phone starts scanning and shows animation window as below picture shows.


Wireless scan in progress

After a few seconds, the phone shows a list of scan result. You can see all the nearby APs using the outer ring of the navigation cluster. To edit an AP, press **Select** to edit it in the **Setup Wi-Fi** page.



In the **Setup Wi-Fi** page, the scanned SSID, security mode, and frequency are displayed. You can enter the credential information, e.g. Passphrase, userid, WEP ...



Setup Wi-Fi

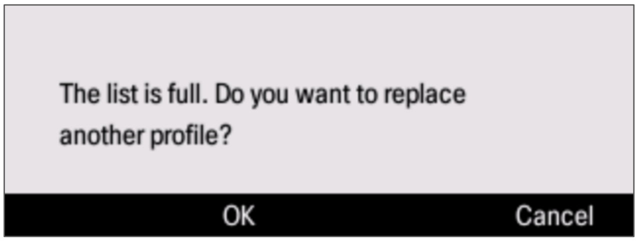
Security mode PSK >

Network name cisco

Passphrase

Once you complete the AP information, you can save the settings as a profile or connect the phone to the AP. When you saved the AP as a profile, you can connect the phone to the saved profile later.

You can save up to 4 profiles to the phone. If all the profiles have AP information configured, the phone pops out an alert message and prompts you to choose replacing a certain profile.



The list is full. Do you want to replace another profile?

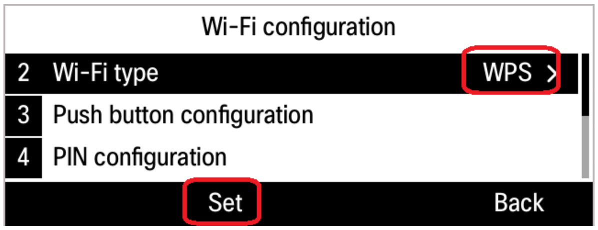
- Automatically connect to a previously connected AP

  When using WLAN type, the phone always tries to recover connection with the last connected AP. In case that the phone is powered off or the AP is shut down, the phone tries to reconnect with the last connected AP first, and will try the other WLAN profiles when fails. The sequence that the phone tries to connect is from profile 1 to profile 4.

Wireless LAN with WPS (on Phone Screen)

The phone supports connecting to a wireless network with WPS. WPS enables the phone to connect to an AP without inputting detailed AP parameters. The WPS connection process is only available on the phone screen menu. There are two ways to transfer secure data with the desired AP: PBC (press button mode) and PIN(pin code mode).

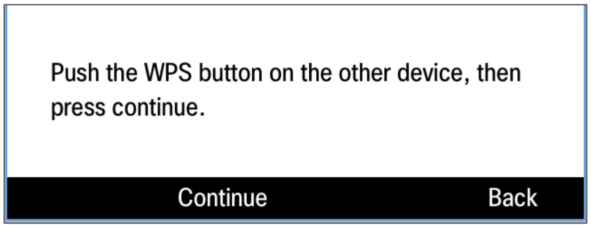
- Set phone to work in WPS type
  Go to **Network configuration > Wi-Fi configuration**. Set **Wi-Fi type** to **WPS** using the selection button and press **Set**. Then **Push button configuration** and **PIN configuration** are displayed.



Wi-Fi configuration

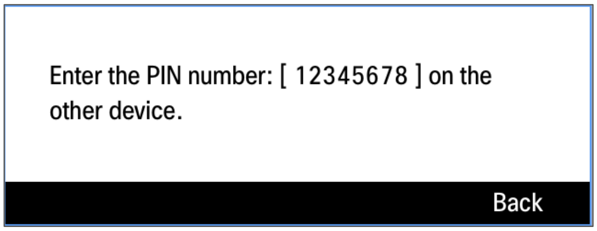
2 Wi-Fi type WPS >

- PBC mode
  Select **Push button configuration** and follow the onscreen instructions. Press the WPS key on the AP and press **Continue** on the phone. The phone starts negotiating with the AP. The process lasts about 2 minutes. The connection status will display on the phone screen.



Push the WPS button on the other device, then press continue.

- PIN mode
  Select **PIN configuration**. A one-time PIN number displays on the phone screen. Enter the PIN number to the AP web page. The phone starts negotiating with the AP. The process lasts about 2 minutes. The connection status will display on the phone screen.



Enter the PIN number: [12345678] on the other device.

- Automatically recover connection to a previously connected AP
  Once the phone talks successfully with the AP via WPS, it can always connect to that AP with learnt info if phone keeps working in WPS type. If Wi-Fi type is changed, the phone cannot recover connection to that WPS AP. You have to reconnect the phone in WPS type manually.

WLAN Connection Troubleshooting

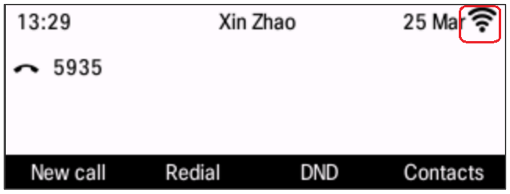
When you encounter a Wi-Fi problem, we suggest that you check the connected AP status, the AP configuration, the Wi-Fi signal strength, and the Wi-Fi messages on the phone. If no issue is detected on the AP and Wi-Fi environment, turn Wi-Fi off and then turn it on again on the phone screen. This could help to recover the Wi-Fi connection. If the problem is still not resolved, report PRT on the phone screen menu or on the phone web page.

You can get the information needed for troubleshooting the WLAN issues by the following means:

- View Wi-Fi status and message on the phone screen
- Capture packets
- Report PRT on the phone or on the phone web page

View Wi-Fi Status and Messages

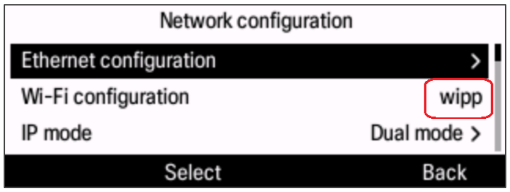
You can view the Wi-Fi connection status and Wi-Fi messages on the phone screen. When the phone is connected to a wireless network, the Wi-Fi signal strength is displayed on the top-right corner of the phone home screen.



13:29 Xin Zhao 25 Mar

5935

You can see the SSID of the connected AP on the **Network configuration** menu.



Network configuration

Ethernet configuration

Wi-Fi configuration: wipp

IP mode: Dual mode

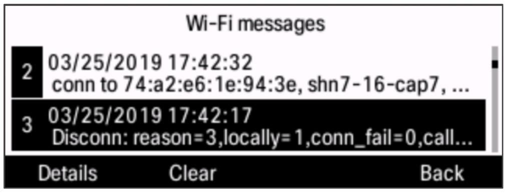
On the **Wi-Fi configuration** menu and its submenus, you can view more details of the connected wireless network.

- Wi-Fi type: Shows the Wi-Fi connection type
- Wi-Fi profile: Contains the connected or saved Wi-Fi profiles
- Wi-Fi status: Shows the connected SSID, the Wi-Fi signal strength, and the MAC address of the AP

To view Wi-Fi messages, go to **Applications** > **Status** > **Wi-Fi messages**.

Wi-Fi messages display the real-time status of Wi-Fi connection. You can use these messages to monitor and troubleshoot Wi-Fi connection issues.

- Details: Extends the selected message to see the full message
- Clear: Clears all the messages
- Back: Returns to the upper level menu


Wi-Fi messages

2 03/25/2019 17:42:32
conn to 74:a2:e6:1e:94:3e, shn7-16-cap7, ...

3 03/25/2019 17:42:17
Disconn: reason=3,locally=1,conn_fail=0,call...

Wi-Fi Message References

The following table describes the Wi-Fi messages and gives suggestions on what to do when you get the messages.

Event	Wi-Fi messages examples on LCD	Event detail and suggested user actions
Connected to an AP	Connected to AP, MAC 00:11:22:33:44:55:66 on channel 36	Shows the AP and the channel that the phone is connected to.
Disconnected from AP	Disconnected: reason=3, locally=0,conn_fail=1,callactive=1	The phone is disconnected from the AP. **Action:** Check the AP and the reason for further debug.
Connection failed	Connection failed	The phone failed to connect with AP. **Action:** Check if Wi-Fi configuration is correct.
Signal strength is low	Wi-Fi signal strength is weaker than -75dBm for more than 12 seconds	Wi-Fi RSSI value is < -75dBm for 12 seconds. **Action:** Check and make sure Wi-Fi signal and environment are good enough.
Firmware memory is low	Wi-Fi firmware memory is low, free/total is xxx/xxx	Wi-Fi firmware memory is low for some reasons. When free memory is less than 50K, it will report this event. Then if the free memory reduces 10k every time, it will report again. When the free memory is less than 25K, the phone reloads Wi-Fi driver. **Action:** This is a warning message. Let the user know that the firmware memory is low.
AP beacon lost	Cannot receive AP signal (BEACON frames), Wi-Fi network may disconnect	The phone can't receive AP's beacon, Wi-Fi will disconnect. **Action:** Check the AP and the environment.
Auth/Assoc not response	Cannot receive AP response for AUTH or ASSOC. Wi-Fi network may disconnect	The phone can't receive response for Wi-Fi authentication or association request, Wi-Fi may disconnect. **Action:** Check the AP and the environment
TX failure, RX undecrypt, channel utilization	TX failure:RX undecrypt:Channel utilization is %d:%d:%d in 2 minutes	The phone gets TX failure, RX undecryption and channel utilization (when the channel utilization is higher than 60%, counter it, if > 100 which is about 10s if beacon is 100ms) in 2 minutes. **Action:** Check and make sure Wi-Fi environment is good enough
WPS fail	WPS connection failed.	WPS connection failed. **Action:** Check if the user configures WPS in the correct way (entering the code within 2 minutes)

Event	Wi-Fi messages examples on LCD	Event detail and suggested user actions
		and no other people are configuring WPS at the same time. If the user connects using PIN mode, make sure that the PIN code is correct.

Capture a Screenshot of the Phone Display

You can capture the current display of the phone.

1. Use your web browser to visit http://<phone_IP_address>/admin/screendump.bmp .

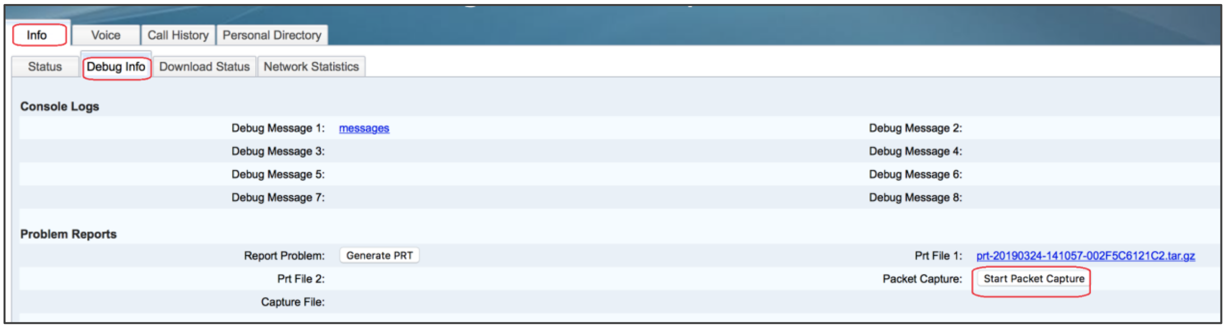
   Example: http://10.79.3.89/admin/screendump.bmp

2. Enter the administrator user name and password when prompted.
3. Capture and save the display using your screenshot tool.
4. To capture another display, switch to the desired menu on the phone and refresh the display in your web browser.

Capture Packets

You can capture the packets sent to and from the phone on the phone's administration web page.

1. Navigate to **Info** > **Debug Info**.
2. In the Problem Reports section, click **Start Packet Capture**.



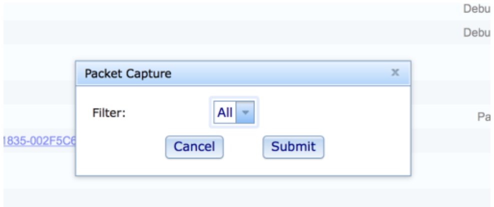
Console Logs

Debug Message 1: messages
Debug Message 2:
Debug Message 3:
Debug Message 4:
Debug Message 5:
Debug Message 6:
Debug Message 7:
Debug Message 8:

Problem Reports

Report Problem: Generate PRT
Prt File 1: prt-20190324-141057-002F5C6121C2.tar.gz
Prt File 2:
Packet Capture: Start Packet Capture
Capture File:

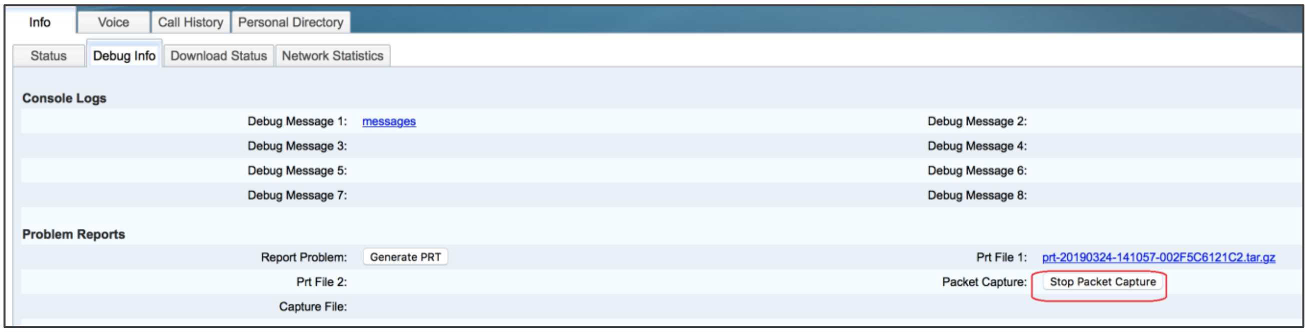
3. Click **Submit** on the prompt.



Packet Capture

Filter: All

4. When finished, click Stop Packet Capture to stop capturing:



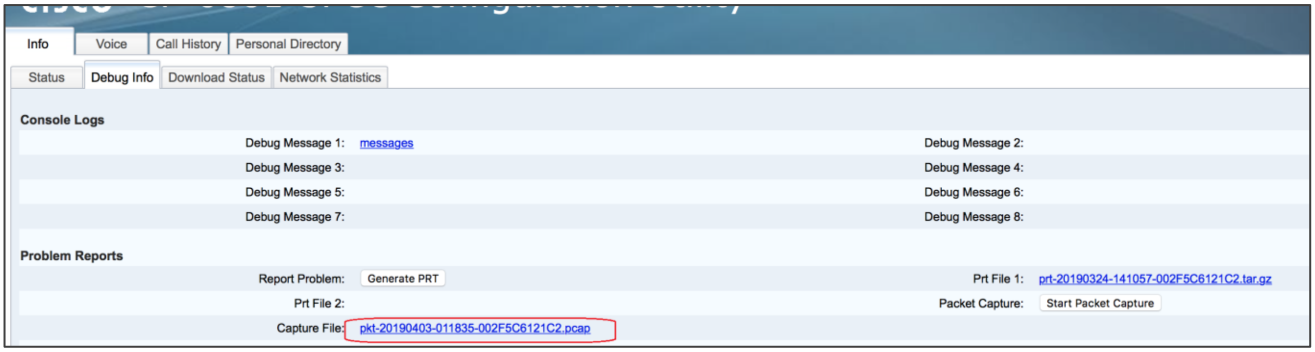
Console Logs

Debug Message 1: messages
Debug Message 2:
Debug Message 3:
Debug Message 4:
Debug Message 5:
Debug Message 6:
Debug Message 7:
Debug Message 8:

Problem Reports

Report Problem: Generate PRT
Prt File 1: prt-20190324-141057-002F5C6121C2.tar.gz
Prt File 2:
Packet Capture: Stop Packet Capture
Capture File:

The captured file is displayed on phone webpage, you can download the file.



Console Logs

Debug Message 1: messages
Debug Message 2:
Debug Message 3:
Debug Message 4:
Debug Message 5:
Debug Message 6:
Debug Message 7:
Debug Message 8:

Problem Reports

Report Problem: Generate PRT
Prt File 1: prt-20190324-141057-002F5C6121C2.tar.gz
Prt File 2:
Packet Capture: Start Packet Capture
Capture File: pkt-20190403-011835-002F5C6121C2.pcap

Report PRT on the Phone

You can use the Problem Reporting Tool (PRT) to collect and send phone logs, and to report problems to your administrator.

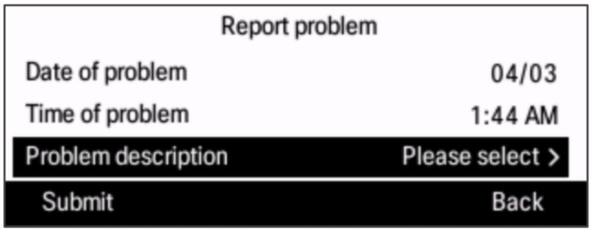
1. Press Applications.

2. Select Status > Report problem.

3. Enter the date that you experienced the problem in the **Date of problem** field. The current date appears in this field by default.

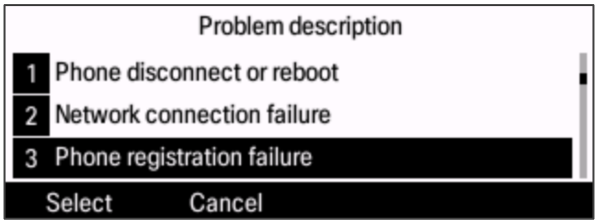
4. Enter the time that you experienced the problem in the **Time of problem** field. The current time appears in this field by default.

5. Select Problem description.


Report problem

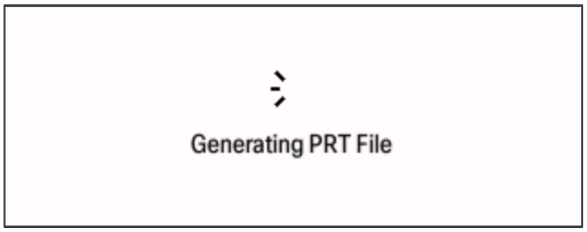
Date of problem 04/03
Time of problem 1:44 AM
Problem description Please select >

6. Select a description from the displayed list.


Problem description

1 Phone disconnect or reboot
2 Network connection failure
3 Phone registration failure

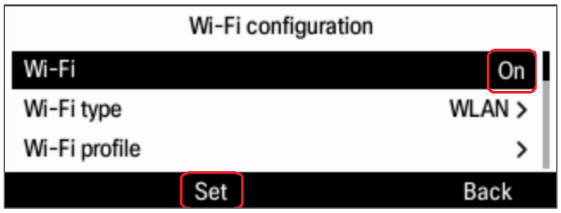
7. Press **Submit**.
The phone starts generating the PRT file. It takes a few seconds for the phone to collect the diagnostic information.



Generating PRT File

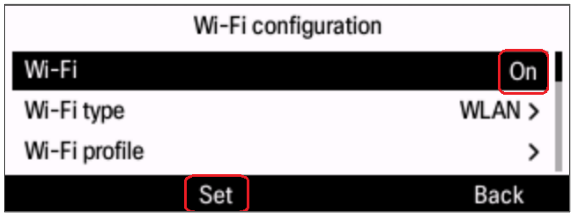
When the PRT file is generated, the phone sends the PRT file to the remote log server which is deployed by SP.

8. In case that phone wifi connection fails, so 6861 phone not able to post PRT to remote server. Please user turn off then on Wi-Fi on LCD. After phone recover the connection, please user proceed with report problem steps.



Wi-Fi configuration

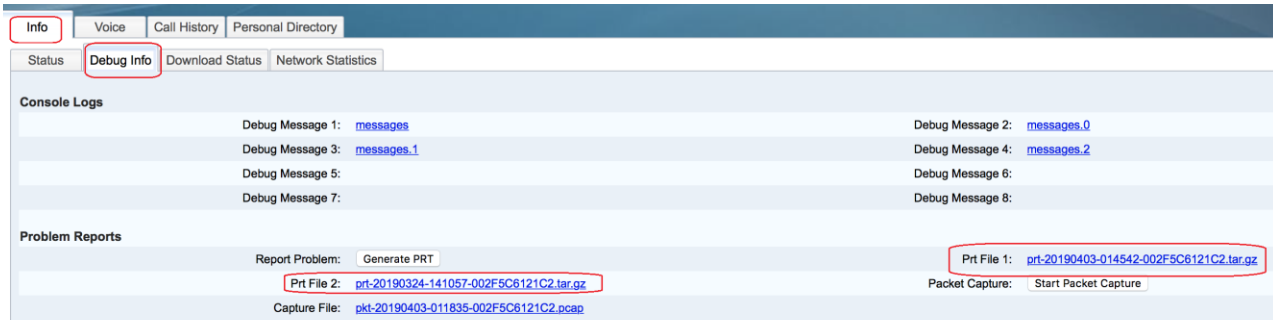
Wi-Fi	On
Wi-Fi type	WLAN >
Wi-Fi profile	>



Wi-Fi configuration

Wi-Fi	On
Wi-Fi type	WLAN >
Wi-Fi profile	>

9. By accessing phone webpage, the PRT files are displayed and downloadable. Totally two PRT files could be saved on phone. They survive the power cycle.



Console Logs

Debug Message 1:	messages	Debug Message 2:	messages.0
Debug Message 3:	messages.1	Debug Message 4:	messages.2
Debug Message 5:		Debug Message 6:	
Debug Message 7:		Debug Message 8:	

Problem Reports

Report Problem:	Generate PRT	Prt File 1:	prt-20190403-014542-002F5C6121C2.tar.gz
Prt File 2:	prt-20190324-141057-002F5C6121C2.tar.gz	Packet Capture:	Start Packet Capture
Capture File:	pkt-20190403-011835-002F5C6121C2.pcap		

Additional Documentation

- Cisco IP Phone 6800 Multiplatform Phones Firmware Data Sheet
- Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide
- Cisco IP Phone 6800 Series Multiplatform Phones User Guide
- Cisco IP Phone 6800 Series Multiplatform Phones Release Notes for Firmware Release 11.2.4
- Cisco Autonomous Access Point Documentation
  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4-25d-JA/Configuration/guide/cg_12_4_25d_JA.html

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’ s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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