Cisco Cius
Wireless Deployment Guide

Cisco Cius is a mobile collaboration tablet built for business. It is designed to help organizations capitalize on the value of mobility by enabling anywhere, anytime access to important business features:

- 7-inch high-resolution multi-touch color display with an intuitive user interface
- Android™ OS 2.2.2
- 1.6 GHz Intel Atom Z615 Processor (512 Kb cache)
- 32 GB eMMC flash memory
- 1 GB RAM
- 4960 mAh removable battery
- Wi-Fi IEEE 802.11 a/b/g/n
- 4G support (HSPA+, W-CDMA, EDGE/GPRS) on Cisco Cius SP model
- Bluetooth 2.1 + EDR (Enhanced Data Rate)
- Micro SD slot and micro USB, micro HDMI and 3.5 mm stereo headphone jack ports
- Forward-facing camera is capable of HD 720p 30-fps video encoding and decoding
- Rear-facing camera is capable of 5 megapixel picture or 720p quality video
- High-definition video interoperability with Cisco TelePresence™ solution and other H.264 video endpoints
- Virtual desktop client integration (VDI) and cloud computing
- Full range of Cisco Collaboration and Unified Communication applications
  Cisco Quad, Cisco WebEx™, Cisco Unified Presence, Instant Messaging, Email, and Cisco Unified Communications Manager voice and video telephony features
- Access to Cisco AppHq and Google Play™
- Expanded Android applications for business, linking Cisco Collaboration APIs through a software developer kit (SDK)
- Accessories including a media station for enhanced capabilities and carrying cases for protection while mobile are sold separately

This guide provides information and guidance to help the network administrator deploy Cisco Cius into a wireless environment.

Revision History

Date	Comments
08/29/11	9.2(1) Release
08/09/12	9.2(2) Release
08/20/13	9.2(3) Release

Contents

Cisco Cius Overview

Cisco Cius is the platform that provides mobile collaboration within enterprises. It brings together the capabilities of Cisco Unified Communication applications, building upon the solid foundations of Cisco Unified Communications devices, both wired and wireless. The levels of multimedia performance that have come to be expected from Cisco products are maintained in Cisco Cius with the introduction of 802.11n data rates and the inclusion of Cisco Compatible eXtensions (CCX).
Cisco's implementation of 802.11, employing CCX, permits time sensitive applications such as voice and video to operate efficiently across campus wide wireless LAN (WLAN) deployments. These extensions provide fast roaming capabilities and an almost seamless flow of multimedia traffic, whilst maintaining security as the end user roams between access points.

It should be understood that WLAN uses unlicensed spectrum, and as a result 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, 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 Cisco Cius in order to take advantage of the 802.11n data rates available. Despite the optimizations that Cisco have implemented in Cisco Cius, the use of unlicensed spectrum means that uninterrupted communication can not be guaranteed, and there may be the possibility of voice or video gaps of up to several seconds during multimedia conversations. Adherence to the deployment guidelines will reduce the likelihood of these voice and video gaps being present, but there is always this possibility. Through the use of unlicensed spectrum, and the inability to guarantee the delivery of messages to a WLAN device, Cisco Cius is not intended as a medical device and should not be used to make clinical decisions.

Requirements

Cisco Cius is an IEEE 802.11a/b/g/n collaboration tablet that provides voice, video, and data communications.

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

Site Survey

Before deploying Cisco Cius into a production environment, a site survey must be completed by a Cisco certified partner with the advanced wireless LAN specialization. During the site survey, the RF (radio frequency) spectrum can be analyzed to determine which channels are usable in the desired band (2.4 GHz or 5 GHz). Typically there is less interference in the 5 GHz band as well as more non-overlapping channels, so 5 GHz is the preferred band for operation and even more highly recommended when Cisco Cius is to be used in a mission critical environment. The site survey will include heatmaps showing the intended coverage plan for the location. The site survey will also determine the access point platform type, antenna type, and access point configuration (channel and transmit power) to use at the location. It is recommended to select an access point with integrated antennas for non-rugged environments (e.g. office, healthcare, education, hospitality) and an access point platform requiring external antennas for rugged environments (e.g. manufacturing, warehouse, retail).
See the Designing the Wireless LAN for Voice section for more information.

Refer to the Steps to Success website for additional information.
http://www.cisco.com/go/stepstosuccess

RF Validation

In order to determine if VoWLAN can be deployed, the environment must be evaluated to ensure the following items meet Cisco guidelines.

Signal

The cell edge should be designed to -67 dBm where there is a 20-30% overlap of adjacent access points at that signal level.

This ensures that Cisco Cius always has adequate signal and can hold a signal long enough in order to roam seamlessly where signal based triggers are utilized vs. packet loss triggers.

Also need to ensure that the upstream signal from Cisco Cius meets the access point's receiver sensitivity for the transmitted data rate. Rule of thumb is to ensure that the received signal at the access point is -67 dBm or higher.

It is recommended to design the cell size to ensure that Cisco Cius can hold a signal for at least 5 seconds.

Channel Utilization

Channel Utilization levels should be kept under 50%.

If using Cisco Cius, this is provided via the QoS Basic Service Set (QBSS), which equates to around 105.

Cisco Cius converts the 0-255 scale to a percentage, so 105 would equate to around 40% in the Cisco Cius neighbor list menu.

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.

Also need to ensure that the upstream signal from Cisco Cius meets the access point's signal to noise ratio for the transmitted data rate.

Packet Loss / Delay

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

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

Retries

802.11 retransmissions should be less than 20%.

Multipath

Multipath should be kept to a minimal as this can create nulls and reduce signal levels.

Many different tools and applications can be used to evaluate these items in order to certify the deployment.

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html
- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html
- Cisco Spectrum Expert

  http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html
- Cisco Unified Operations Manager

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data_sheet_c78-636705.html
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)

  http://www.airmagnet.com

Call Control

Cisco Cius utilizes Session Initiation Protocol (SIP) for call control with the following communications platforms.

- Cisco Unified Communications Manager (CUCM)

  Minimum = 7.1(5)
  Recommended = 7.1(5), 8.5, 8.6, 9.1 and later

Note: Cisco Cius is currently not supported on Cisco Unified Communications Manager Express (CUCME).

Device Support in Cisco Unified Communications Manager

Cisco Unified Communications Manager requires a device package to be installed or service release update in order to enable Cisco Cius device support.

Device packages for Cisco Unified Communications Manager are available at the following location.
http://software.cisco.com/download/navigator.html?mdfid=278875240

Protocols

Supported voice and wireless LAN protocols include the following:

- CCX v5
- Wi-Fi MultiMedia (WMM)
- Unscheduled Auto Power Save Delivery (U-APSD)
- Session Initiation Protocol (SIP)
- Real Time Protocol (RTP)
- G.722, G.711, iSAC, iLBC, G.729, AAC-LD
- H.264
- Real Time Control Protocol (RTCP)
- Cisco Discovery Protocol (CDP)

Access Points

Cisco Cius is supported on both the Cisco Unified and Cisco Autonomous solutions.

Below is the supported version information for each Cisco solution.

- Cisco Unified Wireless LAN Controller

  Minimum = 6.0.202.0 (7.0.116.0 and 7.0.230 are not supported)

  Recommended = 7.0.240.0, 7.2.115.2, 7.3.112.0, 7.4.110.0, 7.5.102.0

- Cisco IOS Access Points (Autonomous)

  Minimum = 12.4(21a)JY

  Recommended = 12.4(25d)JA2, 15.2(2)JB

The supported access point models are listed below.

1040

1140

1250

1260

1600

2600

3500

3600

1130 AG

1240 AG

600

890

Note: Cisco Cius is currently supported with the Cisco AP3600 when the internal 802.11abgn radio is utilized, however is not currently supported in conjunction with the 802.11ac module (AIR-RM3000AC) for the Cisco AP3600.

The table below lists the modes that are supported by each Cisco Access Point.

Cisco AP Series	**802.11a**	**802.11b**	**802.11g**	**802.11n**	**Unified**	**Autonomous**
600	Yes	Yes	Yes	Yes	Yes	No
1040	Yes	Yes	Yes	Yes	Yes	Yes
1130 AG	Yes	Yes	Yes	No	Yes	Yes
1140	Yes	Yes	Yes	Yes	Yes	Yes
1240 AG	Yes	Yes	Yes	No	Yes	Yes
1250	Yes	Yes	Yes	Yes	Yes	Yes
1260	Yes	Yes	Yes	Yes	Yes	Yes
1600	Yes	Yes	Yes	Yes	Yes	Yes
2600	Yes	Yes	Yes	Yes	Yes	Yes

3500	Yes	Yes	Yes	Yes	Yes	Yes
3600	Yes	Yes	Yes	Yes	Yes	Yes
890	Yes	Yes	Yes	Yes	Yes	Yes

Note: VoWLAN is not currently supported in conjunction with outdoor MESH technology (1500 series).

3rd party access points have limited support, as there is no interoperability testing performed against 3rd party access points. However the user should have basic functionality when connected to a Wi-Fi compliant access point.

Cisco Cius can take advantage of Cisco Client Extensions (CCX) enabled access points.

See the following links for more info on CCX.

http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

Antennas

Some of the Cisco Access Points require or allow external antennas.

Please refer to the following URL for the list of supported antennas and how these external antennas should be mounted.

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

3rd party antennas are not supported, as there is no interoperability testing performed against 3rd party antennas including Distributed Antenna Systems (DAS) and Leaky Coaxial Systems.

Please refer to the following URL for more info on Cisco Wireless LAN over Distributed Antenna Systems.

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/positioning_statement_c07-565470.html

Note: The Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i and 3602i Series Access Points are to be mounted on the ceiling as they have omni-directional antennas and are not designed to be patches.

Models

Cisco currently offers a Cisco Cius Wi-Fi only model as well as a Cisco Cius 4G (HSPA+) + Wi-Fi model.

Since there is only a single model for each type of Cisco Cius, an 802.11d enabled access point is required.

Below outlines the modes, frequency ranges and channels supported by each model.

Cisco Cius

Part Number	**Network Mode**	**Frequency Range**	**Available Channels**	**Channel Set**
CIUS-7-K9	Wi-Fi	2.412 – 2.472 GHz 5.180 – 5.240 GHz	13 4	1-13 36,40,44,48

		5.260 – 5.320 GHz 5.500 – 5.700 GHz 5.745 – 5.825 GHz	4 11 5	52,56,60,64 100-140 149,153,157,161,165

Cisco Cius SP

Part Number	**Network Mode**	**Frequency Range**	**Available Channels**	**Channel Set**
CIUS-7-AT-K9	Wi-Fi	2.412 – 2.472 GHz 5.180 – 5.240 GHz 5.260 – 5.320 GHz 5.500 – 5.700 GHz 5.745 – 5.825 GHz	13 4 4 11 5	1-13 36,40,44,48 52,56,60,64 100-140 149,153,157,161,165

Part Number	**Network Mode**	**Network Type**	**Frequency Ranges**
CIUS-7-AT-K9	Mobile	HSPA+ (4G) W-CDMA (3G) EDGE/GPRS (2G)	850 MHz 900 MHz 1800 MHz (EDGE only) 1900 MHz 2100 MHz (HSPA+ and W-CDMA only)

Note: Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

802.11j (Wi-Fi channels 34, 38, 42, 46) are not supported.

Channel 14 for Japan is not supported on the newer Cisco Access Points.

World Mode (802.11d)

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

Cisco Cius requires the access point to be 802.11d enabled, where it can then determine which channels and transmit powers to use.

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 be 802.11h compliant if utilizing those radar frequencies (DFS channels). 802.11h requires 802.11d to be enabled.

Cisco Cius will passively scan DFS channels first before engaging in active scans of those channels.

If using 2.4 GHz (802.11b/g) and 802.11d is not enabled, then Cisco Cius can attempt to use channels 1-11 and reduced transmit power.

Note: World Mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

World Mode must be enabled manually for Cisco Autonomous Access Points using the following commands:

```
Interface dot11radio X
 world-mode dot11d country US both
```

Supported Countries

Below are the countries and their 802.11d codes that are supported by Cisco Cius.

Argentina (AR)
Australia (AU)
Austria (AT)
Belgium (BE)
Brazil (BR)
Bulgaria (BG)
Canada (CA)
Chile (CL)
Colombia (CO)
Costa Rica (CR)
Cyprus (CY)
Czech Republic (CZ)
Denmark (DK)
Estonia (EE)
Finland (FI)
France (FR)
Germany (DE)
Gibraltar (GI)
Greece (GR)
Hong Kong (HK)
Hungary (HU)
Iceland (IS)
India (IN)
Indonesia (ID)
Ireland (IE)
Israel (IL)
Italy (IT)
Japan (JP)
Korea (KR / KP)
Latvia (LV)
Liechtenstein (LI)
Lithuania (LT)
Luxembourg (LU)
Malaysia (MY)
Malta (MT)
Mexico (MX)
Monaco (MC)
Netherlands (NL)
New Zealand (NZ)
Norway (NO)
Oman (OM)
Panama (PA)
Peru (PE)
Philippines (PH)
Poland (PL)
Portugal (PT)
Puerto Rico (PR)
Romania (RO)
Russian Federation (RU)
Saudi Arabia (SA)
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)
Venezuela (VE)
Vietnam (VN)

Note: Compliance information is available on the Cisco Product Approval Status web site at the following URL: http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

Radio Characteristics

The following table lists the data rates, ranges, and receiver sensitivity info for Cisco Cius.

5 GHz Specifications

5 GHz - 802.11a	Data Rate	Modulation	Receiver Sensitivity

Max Tx Power = 16 dBm	6 Mbps	OFDM – BPSK	-91 dBm
	9 Mbps	OFDM – BPSK	-91 dBm
	12 Mbps	OFDM – QPSK	-90 dBm
	18 Mbps	OFDM – QPSK	-88 dBm
	24 Mbps	OFDM – 16 QAM	-85 dBm
	36 Mbps	OFDM – 16 QAM	-81 dBm
	48 Mbps	OFDM – 64 QAM	-77 dBm
	54 Mbps	OFDM – 64 QAM	-76 dBm
5 GHz - 802.11n (20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
20 MHz Channels	7 Mbps (MCS 0)	OFDM – BPSK	-91 dBm
Max Tx Power = 16 dBm	14 Mbps (MCS 1)	OFDM – QPSK	-89 dBm
	21 Mbps (MCS 2)	OFDM – QPSK	-86 dBm
	29 Mbps (MCS 3)	OFDM – 16 QAM	-84 dBm
	43 Mbps (MCS 4)	OFDM – 16 QAM	-81 dBm
	58 Mbps (MCS 5)	OFDM – 64 QAM	-76 dBm
	65 Mbps (MCS 6)	OFDM – 64 QAM	-74 dBm
	72 Mbps (MCS 7)	OFDM – 64 QAM	-72 dBm
5 GHz - 802.11n (40)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
40 MHz Channels	15 Mbps (MCS 0)	OFDM – BPSK	-90 dBm
Max Tx Power = 16 dBm	30 Mbps (MCS 1)	OFDM – QPSK	-87 dBm
	45 Mbps (MCS 2)	OFDM – QPSK	-85 dBm
	60 Mbps (MCS 3)	OFDM – 16 QAM	-81 dBm
	90 Mbps (MCS 4)	OFDM – 16 QAM	-78 dBm
	120 Mbps (MCS 5)	OFDM – 64 QAM	-74 dBm
	135 Mbps (MCS 6)	OFDM – 64 QAM	-72 dBm
	150 Mbps (MCS 7)	OFDM – 64 QAM	-70 dBm

2.4 GHz Specifications

2.4 GHz - 802.11b	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 17 dBm	1 Mbps	DSSS – BPSK	-95 dBm
	2 Mbps	DSSS – QPSK	-93 dBm
	5.5 Mbps	DSSS – CCK	-90 dBm
	11 Mbps	DSSS – CCK	-86 dBm
2.4 GHz - 802.11g	**Data Rate**	**Modulation**	**Receiver Sensitivity**
Max Tx Power = 17 dBm	6 Mbps	OFDM – BPSK	-89 dBm
	9 Mbps	OFDM – BPSK	-89 dBm
	12 Mbps	OFDM – QPSK	-87 dBm
	18 Mbps	OFDM – QPSK	-85 dBm
	24 Mbps	OFDM – 16 QAM	-81 dBm

	36 Mbps	OFDM – 16 QAM	-78 dBm
	48 Mbps	OFDM – 64 QAM	-74 dBm
	54 Mbps	OFDM – 64 QAM	-72 dBm
2.4 GHz - 802.11n (20)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
20 MHz Channels	7 Mbps (MCS 0)	OFDM – BPSK	-88 dBm
Max Tx Power = 17 dBm	14 Mbps (MCS 1)	OFDM – QPSK	-86 dBm
	21 Mbps (MCS 2)	OFDM – QPSK	-84 dBm
	29 Mbps (MCS 3)	OFDM – 16 QAM	-81 dBm
	43 Mbps (MCS 4)	OFDM – 16 QAM	-78 dBm
	58 Mbps (MCS 5)	OFDM – 64 QAM	-73 dBm
	65 Mbps (MCS 6)	OFDM – 64 QAM	-71 dBm
	72 Mbps (MCS 7)	OFDM – 64 QAM	-69 dBm
2.4 GHz - 802.11n (40)	**Data Rate**	**Modulation**	**Receiver Sensitivity**
40 MHz Channels	15 Mbps (MCS 0)	OFDM – BPSK	-85 dBm
Max Tx Power = 17 dBm	30 Mbps (MCS 1)	OFDM – QPSK	-82 dBm
	45 Mbps (MCS 2)	OFDM – QPSK	-80 dBm
	60 Mbps (MCS 3)	OFDM – 16 QAM	-76 dBm
	90 Mbps (MCS 4)	OFDM – 16 QAM	-73 dBm
	120 Mbps (MCS 5)	OFDM – 64 QAM	-69 dBm
	135 Mbps (MCS 6)	OFDM – 64 QAM	-67 dBm
	150 Mbps (MCS 7)	OFDM – 64 QAM	-65 dBm

Note: Receiver sensitivity is the minimum signal needed to decode a packet at a certain data rate.

The above values are pure radio specifications and do not account for the single up to 4 dBi gain integrated antenna.

To achieve 802.11n connectivity, it is recommended that Cisco Cius be within 100 feet of the access point.

See the Designing the Wireless LAN for Voice section for more information on signal requirements.

Language Support

Cisco Cius supports the following languages.

Chinese	German	Portuguese
Czech	Italian	Russian
Dutch	Japanese	Spanish
English	Korean	
French	Polish	

The corresponding locale package must be installed to enable support for that language. English is the default language on Cisco Cius.

Download the locale packages from the Localization page at the following URL:

http://software.cisco.com/download/navigator.html?mdfid=278875240

Mobile Network

Cisco Cius SP supports HSPA+ (4G), W-CDMA (3G), and EDGE (2G) networks.

AT&T is the network provider for Cisco Cius SP.

HSPA+ provides an evolution of High Speed Packet Access and can offer data rates up to 84 Mbps to the mobile device and 22 Mbps from the mobile device when MIMO (multiple antennas) are utilized.

In order to achieve higher data rates, a higher modulation or if dual cell technology (combining multiple cells into one) must be utilized.

The actual speed for a user will be lower than the peak speeds mentioned above. Typically HSPA+ will offer higher connection speeds only when close to the cell tower.

HSPA+ can have a quicker wakeup time, which results as an always-on connection experience.

HSPA+ should not be confused with LTE.

Signal requirements and coverage are to be guaranteed by the service provider.

Audio or video quality over the service provider's mobile network can not be guaranteed.

It is recommended to use 360p or lower quality for video calls over the mobile network.

There is no quality of service (QoS) or call admission control (CAC) across the mobile network including VPN sessions.

There is no support for seamless handoff between mobile networks and Wi-Fi / Ethernet.

- An existing call on the wireless LAN will be not be carried over to the mobile network when roaming out of WLAN coverage unless a VPN session is active. There will be a noticeable audio gap when transitioning from the wireless LAN to the mobile network as the mobile network connection and VPN connection must be established before RTP can resume.
- An existing call can remain up on the mobile network (VPN required) when roaming into coverage of a configured wireless LAN.

Cisco Cius SP supports the following download /uplink speeds and transmit powers.

Mobile Network	Max Data Speeds	Transmit Power
HSPA+	21 Mbps Down/ 5.76 Mbps Up	Max = 24 dBm
W-CDMA	384 Kbps Down / 384 Kbps Up	Max = 24 dBm
EDGE	247 Kbps Down / 247 Kbps Up	Max = 33 dBm

Bluetooth

Cisco Cius supports Bluetooth 2.1 + EDR technology allowing for wireless headset communications.

Bluetooth enables low bandwidth wireless connections within a range of 30 feet, however it is recommended to keep the Bluetooth device within 10 feet of Cisco Cius.

The previously connected device for that Bluetooth profile is given priority.

The Bluetooth device does not need to be within direct line-of-sight of Cisco Cius, but barriers, such as walls, doors, etc. can potentially impact the quality.

Bluetooth utilizes the 2.4 GHz frequency just like 802.11b/g/n and many other devices (e.g. microwave ovens, cordless phones, etc.), so the Bluetooth quality can potentially be interfered with due to using this unlicensed frequency.

Bluetooth Profiles

Cisco Cius supports the following Bluetooth profiles.

Hands-Free Profile (HFP)

With Bluetooth Hands-Free Profile (HFP) support, the following features can be available if supported by the Bluetooth headset.

- Ring
- Answer a call
- End a call
- Volume Control
- Last Number Redial
- Call Waiting
- Divert / Reject
- 3 way calling (Hold & Accept and Release & Accept)
- Speed Dialing

Advanced Audio Distribution Profile (A2DP)

Bluetooth Advanced Audio Distribution Profile (A2DP) support allows for the transfer of a uni-directional high quality stereo audio stream to a Bluetooth enabled stereo headset, car audio system, etc.

Phone Book Access Profile (PBAP)

Phone Book Access Profile (PBAP) support enables the exchange of phone book objects between devices.

PBAP can be utilized by a car kit to display the name of the incoming caller as well as the ability to download the phone book so the user can initiate a call from the car display.

Object Push Profile (OPP)

Object Push Profile (OPP) support enables file sharing between devices.

Objects shared are typically pictures, business cards, meeting details, etc., where the sender initiates the file exchange.

For more information, refer to the documentation from the Bluetooth device manufacturer.

Coexistence (802.11b/g/n + Bluetooth)

If using Coexistence where 802.11b/g/n and Bluetooth are used simultaneously, then there are some limitations and deployment requirements to be considered as they both utilize the 2.4 GHz frequency range.

Capacity

When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced due to the utilization of the 2.4 GHz for both 802.11b/g/n and Bluetooth transmissions.

Multicast Audio

Multicast audio from Push To Talk (PTT), Music on Hold (MMOH) and other applications are not supported when using Coexistence.

Voice Quality

Depending on the current data rate configuration, CTS may be sent to protect the Bluetooth transmissions when using Coexistence.
In some environments, 6 Mbps may need to be enabled.

Note: It is highly recommended to use 802.11a/n if using Bluetooth due to 802.11b/g/n and Bluetooth both utilizing 2.4 GHz, but also due to the above limitations.

Video Calls

Cisco Cius supports video calling via a 7-inch high-resolution multi-touch color LCD and an integrated camera.

The **Video Calling** feature within Cisco Unified Communications Manager must be enabled for each Cisco Cius if wanting to participate in video calls.

Cisco Cius is able to establish video calls with Cisco TelePresence Systems, Cisco Unified IP Phone 8900 and 9900 Series as well as other Cisco Cius endpoints.

360p is the recommended video format to utilize unless HD video is required when communicating with other capable endpoints.

For remote users, 360p should be the maximum video resolution enabled in the Cisco Cius endpoint configuration within Cisco Unified Communications Manager.

A Videoconferencing System with MCU running version 5.7 or later is required to provide videoconferencing capabilities.

A video call can also be established via a VPN session using the Cisco AnyConnect VPN Client.

H.264 is the protocol used for the video stream, where up to 30 fps (frames per second) are supported.

There is a separate stream for the audio session that utilizes one of the support audio codecs.

RTCP in the Cisco Cius configuration within Cisco Unified Communications Manager should be enabled to help sync the audio and video streams.

The following video formats are supported:

- QCIF (176 x 144)
- CIF (352 x 288)
- 360p (640 x 360)
- VGA (640 x 480)
- 720p (1280 x 720)

For more information about Cisco TelePresence, refer to the following URLs:

http://www.cisco.com/en/US/products/ps7060/index.html

For more information about Cisco Unified IP Phone 8900 and 9900 Series, refer to the following URLs:

http://www.cisco.com/en/US/products/ps10451/index.html

http://www.cisco.com/en/US/products/ps10453/index.html

Security

When deploying a wireless LAN, security is essential.

Cisco Cius supports the following wireless security features.

WLAN Authentication

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 and GTC
- CCKM (Cisco Centralized Key Management)
- Open

WLAN Encryption

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

Note: Dynamic WEP with 802.1x authentication and Shared Key authentication are not supported.

Cisco Cius also supports the following additional security features.

- X.509 Digital Certificates
- Image authentication
- Device authentication
- File authentication
- Signaling authentication
- Media encryption (SRTP)
- Signaling encryption (TLS)
- Certificate authority proxy function (CAPF)
- Secure profiles
- Encrypted configuration files
- Screen Lock

- Remote Lock
- Remote Wipe
- Cisco AnyConnect VPN Client

Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling (EAP-FAST)

This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the access point and the Remote Authentication Dial-in User Service (RADIUS) server such as the Cisco Access Control Server (ACS).

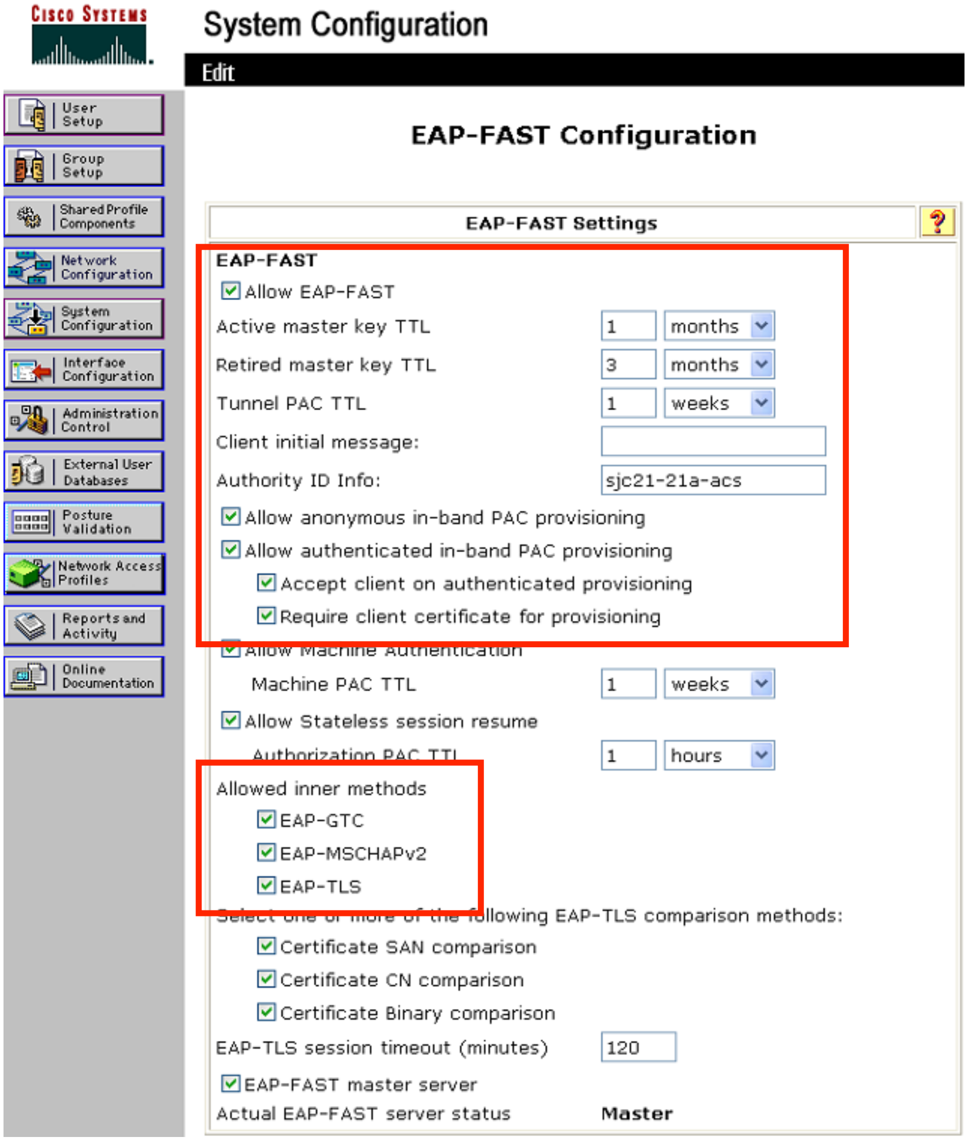
The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (Cisco Cius) and the RADIUS server. The server sends an Authority ID (AID) to the client (Cisco Cius), which in turn selects the appropriate PAC. The client (Cisco Cius) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with its master-key. Both endpoints now have the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but it must enable don the RADIUS server.

To enable EAP-FAST, a certificate must be installed on to the RADIUS server.

Cisco Cius currently supports only automatic provisioning of the PAC, so enable **Allow anonymous in-band PAC provisioning** on the RADIUS server as shown below.

Both EAP-GTC and EAP-MSCHAPv2 must be enabled when **Allow anonymous in-band PAC provisioning** is enabled.

EAP-FAST requires that a user account be created on the authentication server.



EAP-FAST Configuration

EAP-FAST Settings

EAP-FAST

☑ Allow EAP-FAST

Active master key TTL	1	months
Retired master key TTL	3	months
Tunnel PAC TTL	1	weeks
Client initial message:		
Authority ID Info:	sjc21-21a-acs	

☑ Allow anonymous in-band PAC provisioning

☑ Allow authenticated in-band PAC provisioning

☑ Accept client on authenticated provisioning

☑ Require client certificate for provisioning

☑ Allow Machine Authentication

Machine PAC TTL	1	weeks

☑ Allow Stateless session resume

Authorization PAC TTL	1	hours

Allowed inner methods

☑ EAP-GTC

☑ EAP-MSCHAPv2

☑ EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes) 120

☑ EAP-FAST master server

Actual EAP-FAST server status **Master**

If anonymous PAC provisioning is not allowed in the product wireless LAN environment then a staging Cisco ACS can be setup for initial PAC provisioning of Cisco Cius.

This requires that the staging ACS server be setup as a slave EAP-FAST server and components are replicated from the product master EAP-FAST server, which include user and group database and EAP-FAST master key and policy info.

Ensure the production master EAP-FAST ACS server is setup to send the EAP-FAST master keys and policies to the staging slave EAP-FAST ACS server, which will then allow Cisco Cius to use the provisioned PAC in the production environment where **Allow anonymous in-band PAC provisioning** is disabled.

When it is time to renew the PAC, then authenticated in-band PAC provisioning will be used, so ensure that **Allow authenticated in-band PAC provisioning** is enabled.

Ensure that Cisco Cius has connected to the network during the grace period to ensure it can use its existing PAC created either using the active or retired master key in order to get issued a new PAC.

Is recommended to only have the staging wireless LAN pointed to the staging ACS server and to disable the staging access point radios when not being used.

Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)

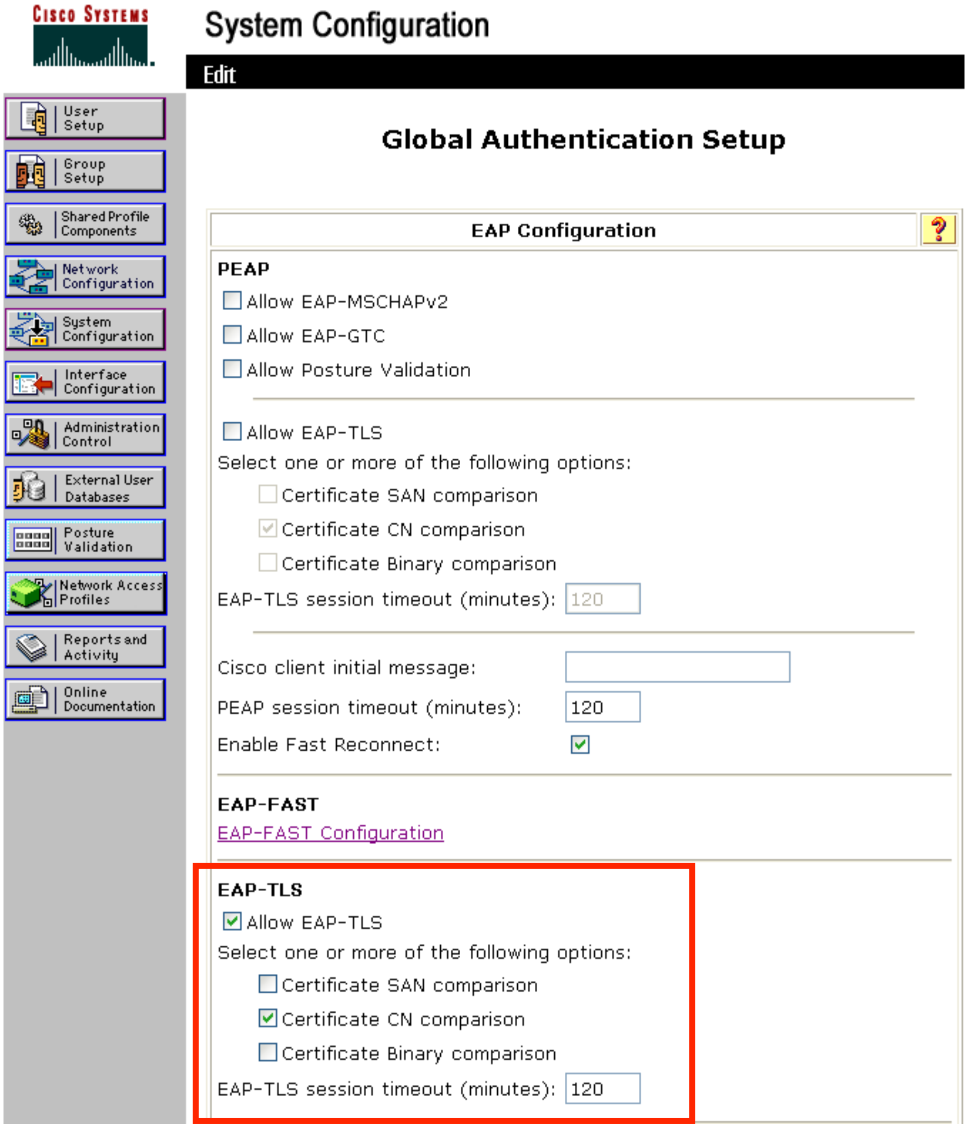
Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

A certificate is required to be installed.

EAP-TLS provides excellent security, but requires client certificate management.

Ensure that **Certificate CN Comparison** is selected when enabling EAP-TLS.



System Configuration

Global Authentication Setup

EAP Configuration

PEAP

□ Allow EAP-MSCHAPv2

□ Allow EAP-GTC

□ Allow Posture Validation

□ Allow EAP-TLS

Select one or more of the following options:

□ Certificate SAN comparison

☑ Certificate CN comparison

□ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

EAP-FAST

EAP-FAST Configuration

EAP-TLS

☑ Allow EAP-TLS

Select one or more of the following options:

□ Certificate SAN comparison

☑ Certificate CN comparison

□ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

EAP-TLS may also require a user account to be created on the authentication server matching the common name of the certificate imported into Cisco Cius.

It is recommended to use a complex password for this user account and that EAP-TLS is the only EAP type enabled on the RADIUS server.

See the Installing Certificates section for more information.

Protected Extensible Authentication Protocol (PEAP)

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.

The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

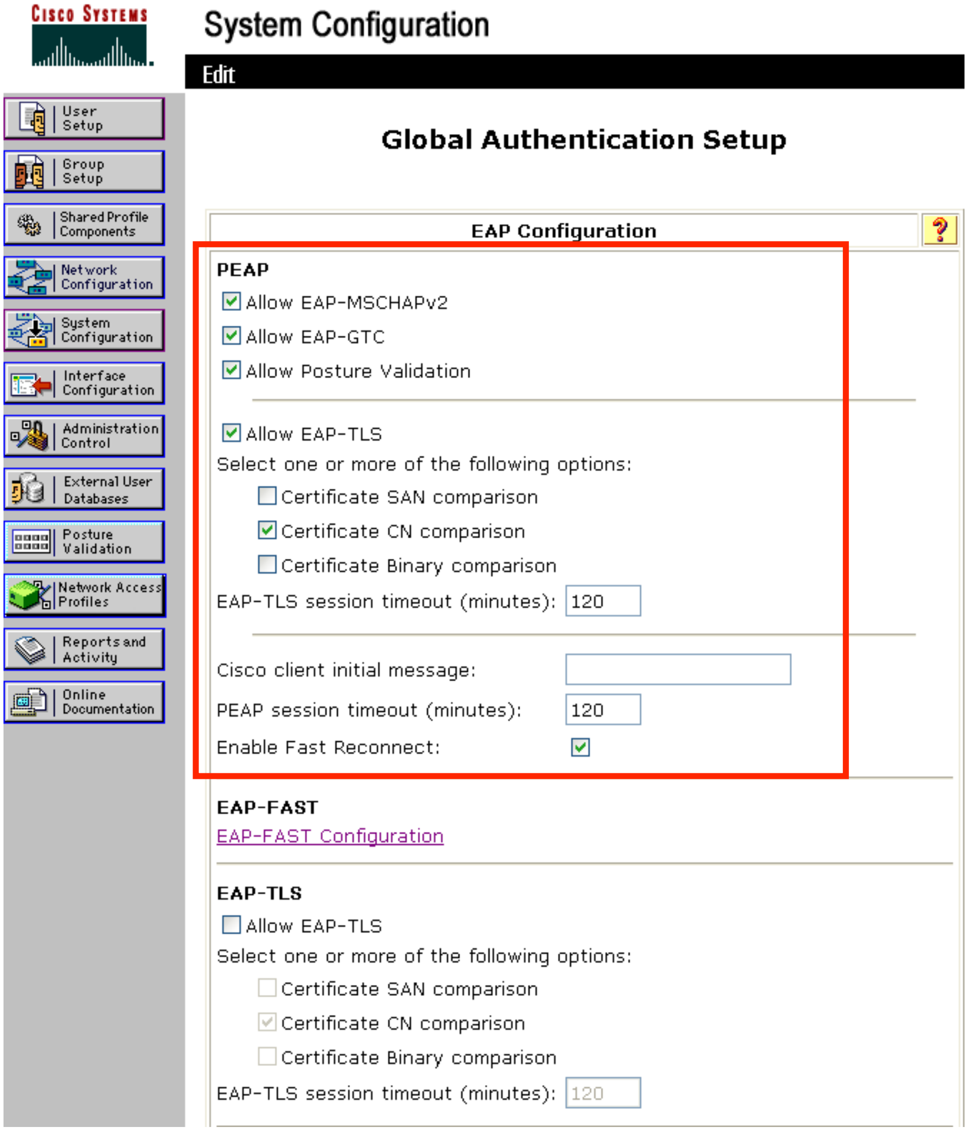
MS-CHAPv2 and GTC are supported inner authentication protocols as of the 9.2(3) release.

PEAP-GTC was not supported prior to the 9.2(3) release.

PEAP requires that a user account be created on the authentication server.

As of the 9.2(3) release, the authentication server can be validated via importing a certificate into Cisco Cius.

See the Installing Certificates section for more information.



System Configuration

Global Authentication Setup

EAP Configuration

PEAP

☑ Allow EAP-MSCHAPv2

☑ Allow EAP-GTC

☑ Allow Posture Validation

☑ Allow EAP-TLS

Select one or more of the following options:

□ Certificate SAN comparison

☑ Certificate CN comparison

□ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

EAP-FAST

EAP-FAST Configuration

EAP-TLS

□ Allow EAP-TLS

Select one or more of the following options:

□ Certificate SAN comparison

☑ Certificate CN comparison

□ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

For more information on Cisco Secure Access Control System (ACS), refer to the following links.

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/ps7032/product_data_sheet09186a00800887d5.html

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/data_sheet_c78-614584.html

Note: If using a firmware release prior to 9.2(3) and a 3rd party RADIUS server, ensure that PEAP v0 (MS-CHAPv2) is enabled. PEAP v1 (GTC) is supported as of the 9.2(3) release.

Cisco Centralized Key Management (CCKM)

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

CCKM enables fast secure roaming and limits the off-network time to keep audio gaps at a minimum when on call.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

CCKM centralizes the key management and reduces the number of key exchanges.

When CCKM is utilized, roaming times can be reduced from 400-500 ms to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

Cisco Cius supports CCKM with WPA2 (AES or TKIP) or WPA (TKIP or AES).

EAP Type	Key Management	Encryption
EAP-FAST	WPA, WPA2	AES, TKIP
EAP-TLS	WPA, WPA2	AES, TKIP
PEAP	WPA, WPA2	AES, TKIP

CCKM is supported with all WPA and WPA2 configurations.

WPA Version	Cipher	Supported
WPA	TKIP	Yes
	AES	Yes
WPA2	TKIP	Yes
	AES	Yes

EAP and User Database Compatibility

The following chart displays the EAP and database configurations supported by Cisco Cius.

Database Type	EAP-FAST (Phase Zero)	EAP-TLS	PEAP (GTC)	PEAP (MS-CHAPv2)
Cisco ACS	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	Yes	Yes

Windows AD	Yes	Yes	Yes	Yes
LDAP	No	Yes	Yes	No
ODBC (ACS for Windows Only)	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	Yes	Yes
All Token Servers	No	No	No	No

Power Management

Cisco Cius has a 4960 mAh / 18.4 Wh removal battery that is intended to provide at least 8 hours of talk time.

When the access point supports the Cisco Client Extensions (CCX) proxy ARP information element, the idle battery life will be optimized. Proxy ARP allows Cisco Cius to remain in sleep mode longer versus waking up at each Delivery Traffic Indicator Message (DTIM) period to check for incoming broadcasts.

To optimize battery life, Cisco Cius will utilize either U-APSD or PS-POLL depending on whether Wi-Fi MultiMedia (WMM) is enabled in the Access Point configuration or not.

U-APSD will be utilized when WMM is enabled on the Access Point.

Active mode can also be utilized in some certain situations.

Battery life can be reduced when on call and using Coexistence (802.11b/g/n + Bluetooth).

If the access point does not support CCX or proxy ARP is not enabled, then the idle battery life will be up to fifty percent less. See the Configuring Proxy ARP section for more information.

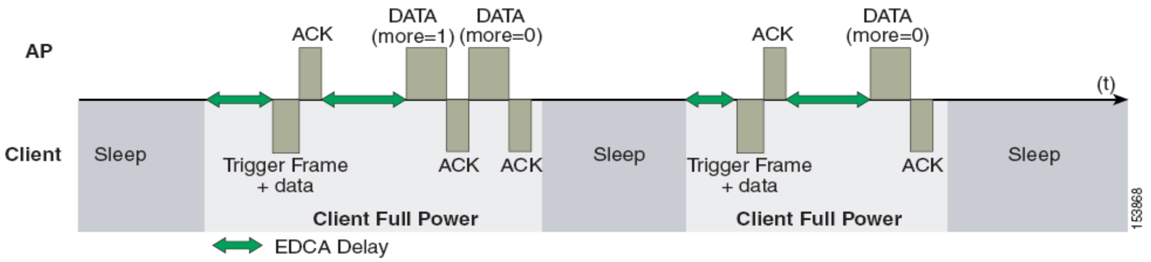
Protocols

Unscheduled Auto Power Save Delivery (U-APSD)

Cisco Cius will utilize U-APSD (Unscheduled Auto Power Save Delivery) for power management as long as Wi-Fi MultiMedia (WMM) is enabled in the access point configuration.

U-APSD helps optimize battery life and reduces management overhead.

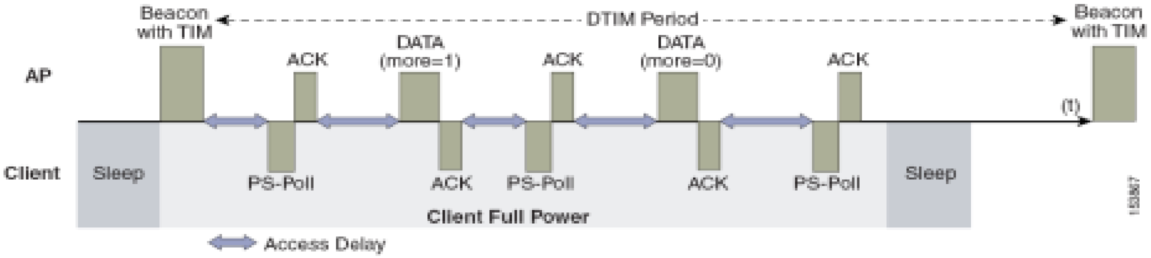
Below is a sample packet sequence when using U-APSD.



Power Save Poll (PS-POLL)

If WMM is disabled (disabling U-APSD support) or U-APSD support is not available on the access point, then Cisco Cius will utilize PS-POLL for power management.

Below is a sample packet sequence when using PS-POLL.



Delivery Traffic Indicator Message (DTIM)

Cisco Cius can use the DTIM period to schedule wake up periods to check for broadcast and multicast packets as well as any unicast packets.

If proxy ARP is enabled, then Cisco Cius does not have to wake up at DTIM.

For optimal battery life and performance, it is recommended to set the DTIM period to **2** with a beacon period of **100 ms**.

The DTIM period is a tradeoff between battery life and multicast performance.

Broadcast and multicast traffic will be queued until the DTIM period when there are power save enabled clients associated to the access point, so DTIM will determine how quickly these packets can be delivered to the client. If using multicast applications, a shorter DTIM period can be used.

If multiple multicast streams exist on the wireless LAN frequently, then it is recommended to set the DTIM period to **1**.

Quality of Service (QoS)

Quality of Service enables queuing to ensure high priority for voice and video traffic.

To enable proper queuing for voice, interactive video, and call control traffic use the following guidelines.

- Ensure that **WMM** is enabled on the access point.
- Create a QoS policy on the access point giving priority to voice, interactive video, and call control traffic.

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384 - 32767
Interactive Video & Audio for Video Calls	AF41 (34)	4	5	UDP 16384 - 32767
Call Control	CS3 (24)	3	4	TCP 5060 - 5061

- Be sure that voice, interactive video, and call control packets have the proper QoS markings and other protocols are not using the same QoS markings.

- Select the **Platinum** QoS profile for the voice wireless LAN when using Cisco Unified Wireless LAN Controller technology and set the 802.1p tag to **6.**
- Enable Differentiated Services Code Point (DSCP) preservation on the Cisco IOS switch.

Note: Voice and interactive video frames will be marked with DSCP AF41 and WMM UP 5 for video calls.

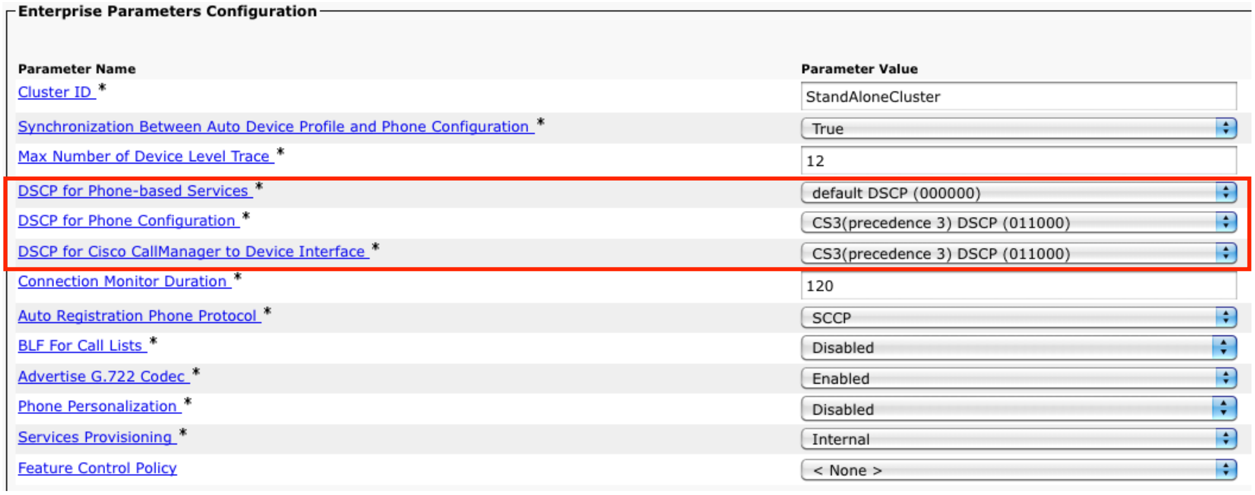
The WMM UP marking could be downgraded if CAC (TSPEC) is enabled for voice or video.

For more information about TCP and UDP ports used by Cisco Cius and the Cisco Unified Communications Manager, refer to the Cisco Unified Communications Manager TCP and UDP Port Usage document at this URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/8_6_1/portlist861.html

Configuring QoS in Cisco Unified Communications Manager

The SIP DSCP values are configured in the Cisco Unified Communications Manager enterprise parameters. Cisco Unified Communications Manager uses the default value of CS3 to have devices set the DSCP marking for SIP packets as shown in the Enterprise Parameters Configuration page.



Enterprise Parameters Configuration

Parameter Name	Parameter Value
Cluster ID *	StandAloneCluster
Synchronization Between Auto Device Profile and Phone Configuration *	True
Max Number of Device Level Trace *	12
DSCP for Phone-based Services *	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120
Auto Registration Phone Protocol *	SCCP
BLF For Call Lists *	Disabled
Advertise G.722 Codec *	Enabled
Phone Personalization *	Disabled
Services Provisioning *	Internal
Feature Control Policy	< None >

Configuring QoS Policies for the Network

Configure QoS policies and settings for the following network devices.

Configuring Cisco Switch Ports

Configure the Cisco Unified Wireless LAN Controller and Cisco Access Point switch ports as well as any uplink switch ports.

Configure the Cisco Unified Wireless LAN Controller for trust COS.

Below is a sample switch configuration for the Cisco Unified Wireless LAN controller:

```
mls qos
!
```

```
interface X
 mls qos trust cos
```

Configure the Cisco Access Point switch ports as well as any uplink switch ports for trust DSCP.

Below is a sample switch configuration for an access point:

```
mls qos
!
interface X
 mls qos trust dscp
```

Note: When using the Cisco Unified Wireless LAN Controller, DSCP trust must be implemented or trust the UDP data ports used by the Cisco Unified Wireless LAN Controller (CAPWAP = 5246 and 5247) on all interfaces where wireless packets will traverse to ensure QoS markings are correctly set.

Configuring Cisco IOS Access Points

Use the following QoS policy on the Cisco IOS Access Point (AP) to enable DSCP to CoS (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.

```
class-map match-all Voice
 match ip dscp ef
class-map match-all Video
 match ip dscp af41
class-map match-all CallControl
 match ip dscp cs3
!
policy-map Cius
 class Voice
  set cos 6
class Video
  set cos 5
 class CallControl
  set cos 4
!
interface dot11radioX
 service-policy input Cius
 service-policy output Cius
```

Configuring Switch Ports for Wired IP Phones

Enable the Cisco wired IP phone switch ports for Cisco phone trust.

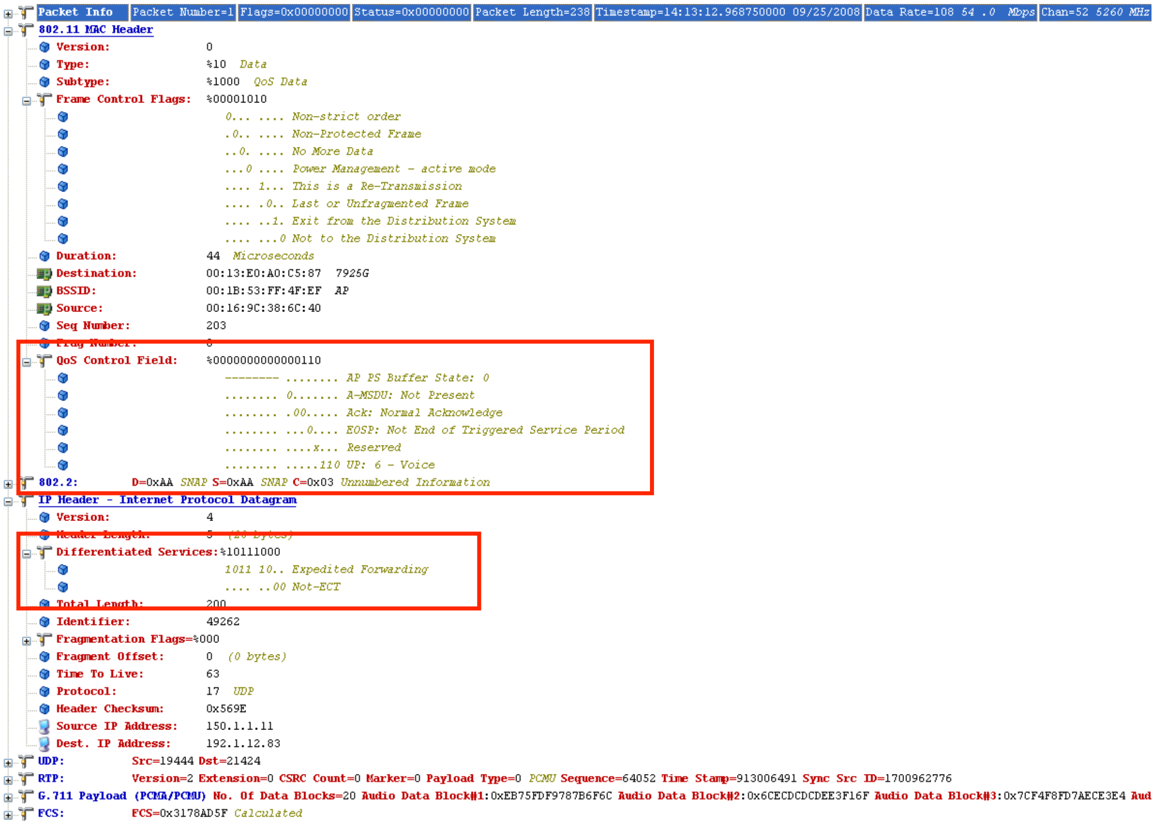
Below is a sample switch configuration:

```
mls qos
!
Interface X
 mls qos trust device cisco-phone
 mls qos trust dscp
```

Sample Voice Packet Capture

The packet capture below displays a voice packet bound for Cisco Cius over the air being marked as DSCP = EF and UP = 6.

This would require that admission control mandatory to be disabled for voice, otherwise the voice frame would be downgraded to a lower user priority (UP) since Cisco Cius does not currently support TSPEC.



```
Packet Info   Packet Number=1 Flags=0x00000000 Status=0x00000000 Packet Length=238 Timestamp=14:13:12.968750000 09/25/2008 Data Rate=108 54 .0  Mbps Chan=52 5260 MHz
802.11 MAC Header
   Version:              0
   Type:                 %10  Data
   Subtype:              %1000  QoS Data
   Frame Control Flags:  %00001010
                            0... .... Non-strict order
                            .0.. .... Non-Protected Frame
                            ..0. .... No More Data
                            ...0 .... Power Management - active mode
                            .... 1... This is a Re-Transmission
                            .... .0.. Last or Unfragmented Frame
                            .... ..1. Exit from the Distribution System
                            .... ...0 Not to the Distribution System
   Duration:             44  Microseconds
   Destination:          00:13:E0:A0:C5:87  7925G
   BSSID:                00:1B:53:FF:4F:EF  AP
   Source:               00:16:9C:38:6C:40
   Seq Number:           203
   Frag Number:          0
   QoS Control Field:    %0000000000000110
                            -------- ........ AP PS Buffer State: 0
                            ........ 0....... A-MSDU: Not Present
                            ........ .00..... Ack: Normal Acknowledge
                            ........ ...0.... EOSP: Not End of Triggered Service Period
                            ........ ....x... Reserved
                            ........ .....110 UP: 6 - Voice
802.2:        D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information
IP Header - Internet Protocol Datagram
   Version:              4
   Header Length:        5  (20 bytes)
   Differentiated Services:%10111000
                            1011 10.. Expedited Forwarding
                            .... ..00 Not-ECT
   Total Length:         200
   Identifier:           49262
   Fragmentation Flags=%000
   Fragment Offset:      0  (0 bytes)
   Time To Live:         63
   Protocol:             17  UDP
   Header Checksum:      0x569E
   Source IP Address:    150.1.1.11
   Dest. IP Address:     192.1.12.83
UDP:          Src=19444 Dst=21424
RTP:          Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=0 PCMU Sequence=64052 Time Stamp=913006491 Sync Src ID=1700962776
G.711 Payload (PCMA/PCMU) No. Of Data Blocks=20 Audio Data Block#1:0xEB75FDF9787B6F6C Audio Data Block#2:0x6CECDCDCDEE3F16F Audio Data Block#3:0x7CF4F8FD7AECE3E4 Aud
FCS:          FCS=0x3178AD5F Calculated
```

Call Admission Control

Cisco Cius currently does not support TSPEC for Call Admission Control of voice or video streams.

If TSPEC is enabled for voice or video in the access point, then the priority of voice and video frames will be downgraded.

Without TSPEC support, TCLAS is also not supported.

Since TSPEC is not supported at this time, SIP CAC and media session snooping can optionally be enabled on the Cisco Unified Wireless LAN Controller.

See the Configuring the Cisco Unified Wireless LAN Controller and Access Points section for more info including the pros and cons for enabling SIP CAC.

Roaming

CCKM is the recommended deployment model for all environment types where frequent roaming occurs.

802.1x authentication is required in order to utilize CCKM.

802.1x without CCKM can introduce delay during roaming due to its requirement for full re-authentication. WPA and WPA2 introduce additional transient keys and can lengthen roaming time.

When CCKM is utilized, roaming times can be reduced from 400-500 ms to less than 100 ms, where that transition time from one access point to another will not be audible to the user.

Cisco Cius supports CCKM with WPA2 (AES or TKIP) or WPA (TKIP or AES).

Authentication	Roaming Time
WPA/WPA2 Personal	150 ms
WPA/WPA2 Enterprise	300 ms
CCKM	< 100 ms

Cisco Cius manages the scanning and roaming events; Client Roaming parameters in the Cisco Unified Wireless LAN Controller are not utilized.

Roaming can be triggered for either of the following reasons.

- RSSI Differential
- Max Tx Retransmissions (not receiving 802.11 acknowledgements from the access point)
- Missed Beacons

The roaming trigger for the majority of roams should be due to meeting the required RSSI differential based on the current RSSI, which results in seamless roaming (no voice or video interruptions).

Unexpected roams are triggered either by missing contiguous 802.11 acknowledgements (Max Tx retransmissions) or beacons from the access point.

For seamless roaming to occur, Cisco Cius must be associated to an access point for at least 3 seconds, otherwise roams can occur based on packet loss (max tx retransmissions or missed beacons).

Roaming based on RSSI may not occur if the current signal has met the strong RSSI threshold.

Note: Cisco Cius does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Interband Roaming

Cisco Cius defaults to Auto for frequency band mode, which enables interband roaming and gives preference to the strongest signal. Typically this will give preference to 2.4 GHz over 5 GHz due to 2.4 GHz having a stronger signal in general assuming the power levels are the same.

At power on, Cisco Cius will scan all 2.4 GHz and 5 GHz channels when in Auto band mode, then attempt to associate to an access point using the locally configured network settings. In Auto mode, Cisco Cius scans both bands simultaneously regardless of call state to allow for seamless interband roaming. Cisco Cius will list the neighbors by the current signal strength where the frequency band is not a factor.

If configured for 5 GHz only or 2.4 GHz only mode, then just those channels are scanned.

It is recommended to perform a spectrum analysis to ensure that the desired bands can be enabled in order to perform interband roaming.

Multicast

When enabling multicast in the wireless LAN, performance and capacity must be considered.

If there is an associated client that is in power save mode, then all multicast packets will be queued until the DTIM period.

If proxy ARP from CCX is enabled and Cisco Cius is not participating in a multicast session currently, then the access point is responsible to answer any ARP requests on behalf of the client and Cisco Cius can remain in sleep mode longer thus optimizing battery life.

If there are many packets queued up, then they client may have to stay awake longer thus potentially reducing battery life.

With multicast, there is no guarantee that the packet will be received the by the client.

The multicast traffic will be sent at the highest mandatory / basic data rate enabled on the access point, so will want to ensure that only the lowest enabled rate is configured as the only mandatory / basic rate.

The client will send the IGMP join request to receive that multicast stream. The client will send the IGMP leave when the session is to be ended.

Cisco Cius supports the IGMP query feature, which can be used to reduce the amount of multicast traffic on the wireless LAN when not necessary.

Ensure that IGMP snooping is also enabled on all switches.

It is recommended to enable Multicast Direct in the Cisco Unified Wireless LAN Controller.

Note: If using Coexistence where 802.11b/g/n and Bluetooth are being used simultaneously, then multicast voice is not supported.

Designing the Wireless LAN

The following network design guidelines must be followed in order to accommodate for adequate coverage, call capacity and seamless roaming for Cisco Cius.

Planning Channel Usage

Use the following guidelines to plan channel usage for these wireless environments.

5 GHz (802.11a/n)

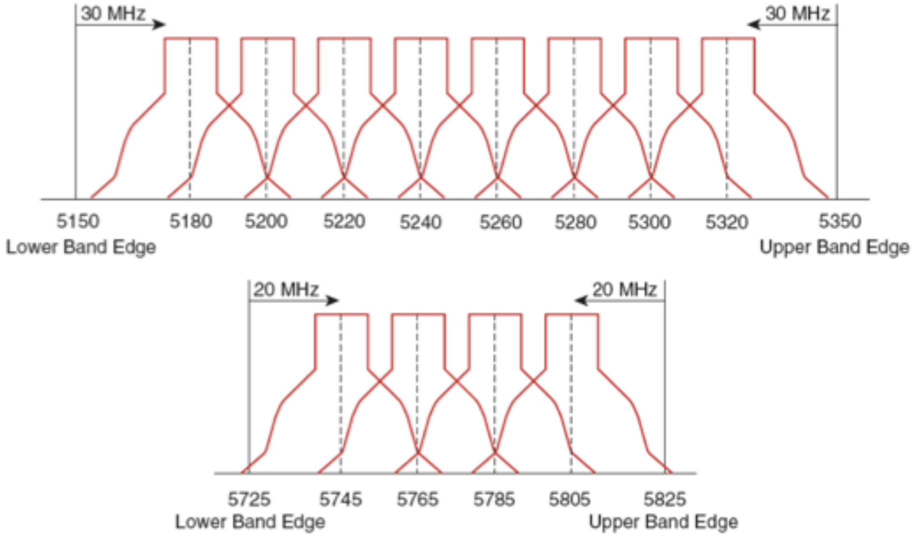
Cisco Cius supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) from 802.11h, which are required when using channels operating at 5.260 - 5.700 GHz (15 of the 24 possible channels).

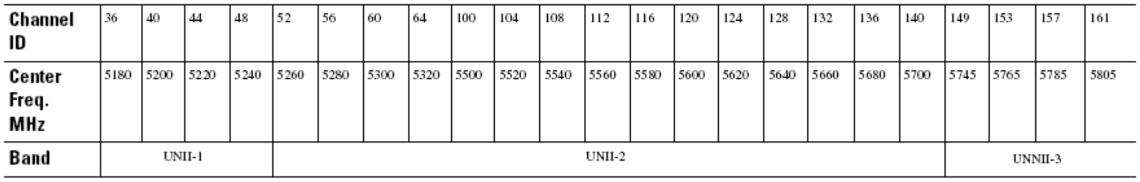
DFS dynamically instructs a transmitter to switch to another channel whenever radar signal is detected. If the access point detects radar, the radio on the access point goes on hold for at least 60 seconds while the access point passively scans for another usable channel.

TPC allows the client and access point to exchange information, so that the client can dynamically adjust the transmit power. The client uses only enough energy to maintain association to the access point at a given data rate. As a result, the client contributes less to adjacent cell interference, which allows for more densely deployed, high-performance wireless LANs.

5 GHz channels overlap their adjacent channel, so there should be at least 1 channel of separation for adjacent access points.

Need to ensure there is at least 20 percent overlap with adjacent channels when deploying Cisco Cius in the 802.11a/n environment, which allows for seamless roaming. For critical areas, it is recommended to increase the overlap (30% or more) to ensure that there can be at least 2 access points available with a signal of-67 dBm or higher, while Cisco Cius also meets the access point's receiver sensitivity (required signal level for the current data rate).





Channel ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
Center Freq. MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805
Band	UNII-1				UNII-2															UNNII-3			

Using Dynamic Frequency Selection (DFS) on Access Points

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).

For Cisco Unified Access Points, enable Auto RF unless there is an intermittent interferer in an area, which select access points can have the channel statically assigned.

If there are repeated radar events detected by the access point (just or falsely), determine if the radar signals are impacting a single channel (narrowband) or multiple channels (wideband), then potentially disable use of that channel or channels in the wireless LAN.

The presence of an AP on a non-DFS channel can help minimize voice interruptions.

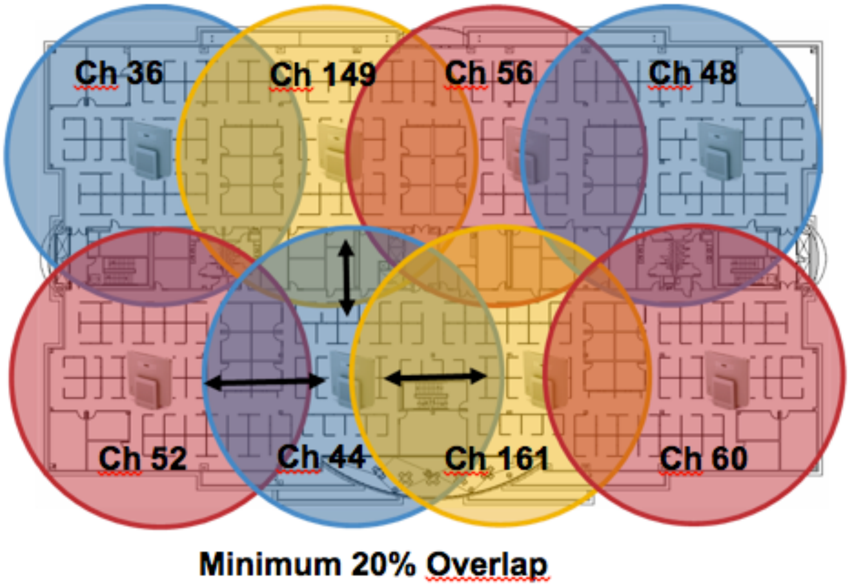
In case of radar activity, have at least one access point per area that uses a non-DFS channel (UNII-1). This ensures that a channel is available when an access point's radio is in its hold-off period while scanning for a new usable channel.

For Cisco Autonomous Access Points, enable band 1 only, which allows the access point to use only a UNII-1 channel.

For Cisco Unified Access Points, can manually select a UNII-1 channel (channels 36, 40, 44, 48) for the desired access points.

A UNII-3 channel (5.745 - 5.825 GHz) can optionally be used if available.

In this diagram, 5 GHz cells use a non-DFS channel while other nearby cells use DFS channels to permit maximum call capacity under all conditions.

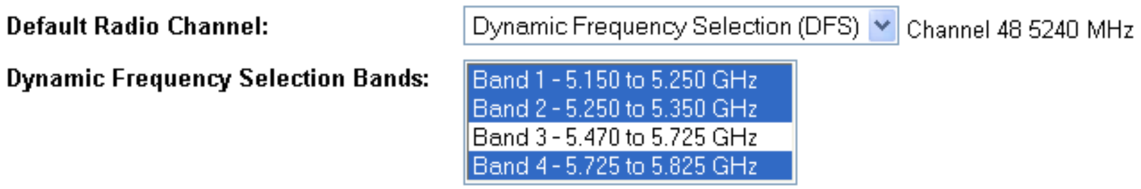


For 5 GHz, 21 channels are available in the Americas and 16 channels in Europe and Japan.

Where UNII-3 is available, it is recommended to use UNII-1, UNII-2, and UNII-3 only to utilize a 12 channel set.

If planning to use UNII-2 extended channels (channels 100 - 140), it is recommended to disable UNII-2 (channels 52-64) on the access point to avoid having so many channels enabled.

Having many 5 GHz channels enabled in the wireless LAN can delay discovery of new access points.



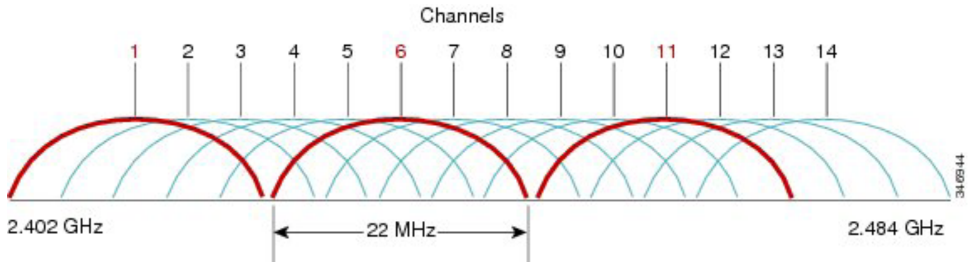
Default Radio Channel: Dynamic Frequency Selection (DFS) Channel 48 5240 MHz

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

2.4 GHz (802.11b/g/n)

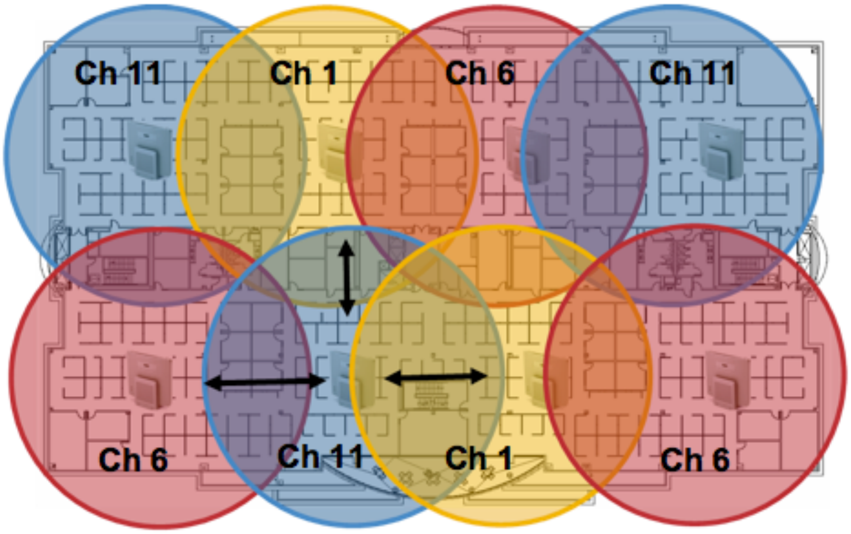
In the 2.4 GHz (802.11b/g/n environment, only non-overlapping channels must be utilized when deploying VoWLAN. Non-overlapping channels have 22 MHz of separation and are at least 5 channels apart.

There are only 3 non-overlapping channels in the 2.4 GHz frequency range (channels 1, 6, 11).



Non-overlapping channels must be used and allow at least 20 percent overlap with adjacent channels when deploying Cisco Cius in the 802.11b/g/n environment, which allows for seamless roaming.

Using an overlapping channel set such as 1, 5, 9, 13 is not a supported configuration.



Minimum 20% Overlap

Signal Strength and Coverage

To ensure acceptable voice quality, Cisco Cius should always have a signal of -67 dBm or higher when using 2.4 GHz or 5 GHz, while Cisco Cius also meets the access point's receiver sensitivity required signal level for the transmitted data rate.

Ensure the Packet Error Rate (PER) is no higher than 1%.

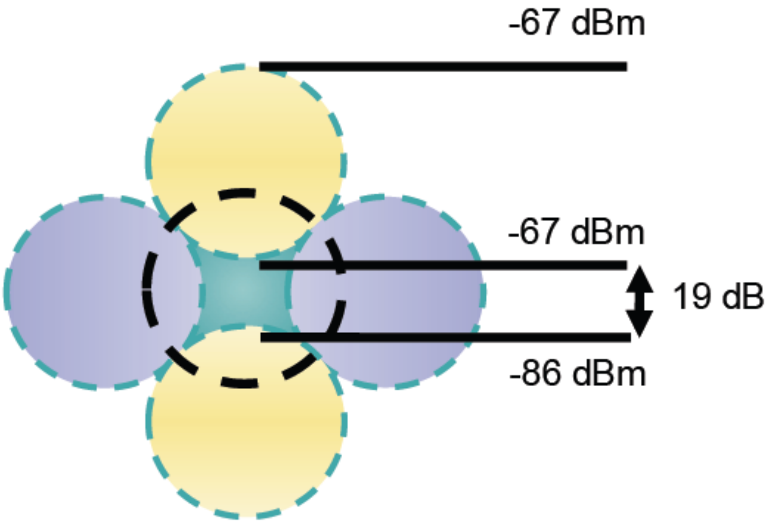
A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm signal should be maintained.

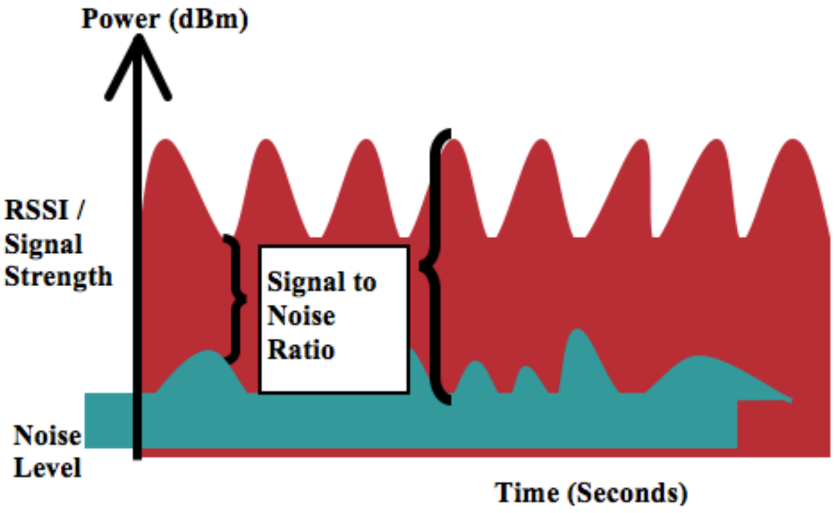
It is recommended to have at least two access points on non-overlapping channels with at least -67 dBm signal with the 25 dB SNR to provide redundancy.

To achieve maximum capacity and throughput, the wireless LAN should be designed to 24 Mbps. Higher data rates (36-54 Mbps) can optionally be enabled for other applications other than voice only that can take advantage of these higher data rates.

Recommended to set the minimum data rate to 11 Mbps or 12 Mbps for 2.4 GHz (dependent upon 802.11b client support policy) and 12 Mbps for 5 GHz, which should also be the only rate configured as a mandatory / basic rate.
In some environments, 6 Mbps may need to be enabled as a mandatory / basic rate.

Due to the above requirements, a single channel plan should not be deployed.





When designing the placement of access points, be sure that all key areas have sufficient coverage (signal).

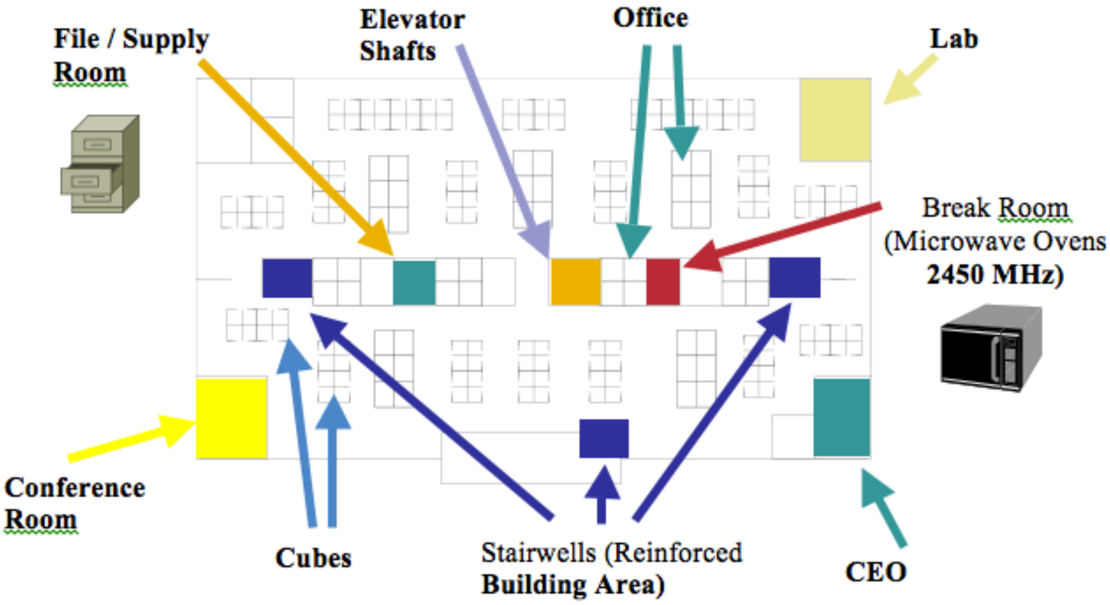
Typical wireless LAN deployments for data only applications do not provide coverage for some areas where VoWLAN service is necessary such as elevators, stairways, and outside corridors.

Wireless LAN interference is generated by microwave ovens, 2.4 GHz cordless phones, Bluetooth devices, or other electronic equipment operating in the 2.4 GHz band.

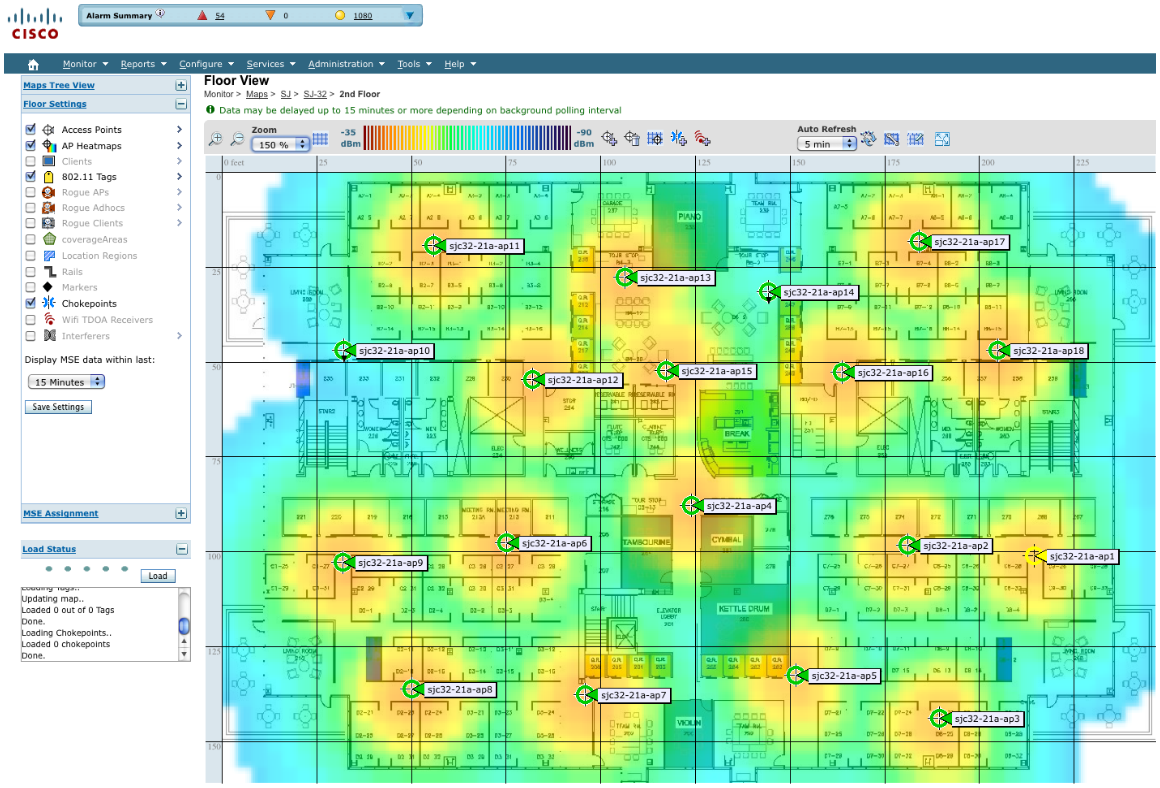
Microwave ovens operate on 2450 MHz, which is between channels 8 and 9 of 802.11b/g/n. Some microwaves are shielded more than others and that shielding reduces the spread of the energy. Microwave energy can impact channel 11, and some microwaves can affect the entire frequency range (channels 1 through 11). To avoid microwave interference, select channel 1 for use with access points that are located near microwaves.

Most microwave ovens, Bluetooth, and frequency hopping devices do not have the same effect on the 5 GHz frequency. The 802.11a/n technology provides more non-overlapping channels and typically lower initial RF utilization. For voice deployments, it is suggested to use 802.11a/n for voice and use 802.11b/g/n for data.

However there are products that also utilize the non-licensed 5 GHz frequency (e.g. 5.8 GHz cordless phones, which can impact UNII-3 channels).


File / Supply Room
Elevator Shafts
Office
Lab
Break Room (Microwave Ovens 2450 MHz)
Conference Room
Cubes
Stairwells (Reinforced Building Area)
CEO

The Cisco Unified WCS or NCS can be utilized to verify signal strength and coverage.



Floor View

Monitor > Maps > SJ > SJ-32 > 2nd Floor

Data may be delayed up to 15 minutes or more depending on background polling interval

Zoom: 150 %

Auto Refresh: 5 min

- ☑ Access Points
- ☑ AP Heatmaps
- □ Clients
- ☑ 802.11 Tags
- □ Rogue APs
- □ Rogue Adhocs
- □ Rogue Clients
- □ coverageAreas
- □ Location Regions
- □ Rails
- □ Markers
- ☑ Chokepoints
- □ Wifi TDOA Receivers
- □ Interferers

Display MSE data within last: 15 Minutes

Save Settings

```
Updating map..
Loaded 0 out of 0 Tags
Done.
Loading Chokepoints..
Loaded 0 chokepoints
Done.
```

Configuring Data Rates

It is recommended to disable rates below 12 Mbps for 802.11a/n deployments and for 802.11g/n deployments where capacity and range are factored in for best results.

Cisco Cius has a single antenna, therefore it supports up to MCS 7 data rates for 802.11n connectivity (up to 72 or 150 Mbps depending on the channel width utilized).

MCS 8 - MCS 15 rates can be left enabled for other 802.11n clients, which are utilizing the same band frequency and utilize MIMO (multiple input / multiple output) antenna technology, which can take advantage of those higher rates.

If 802.11b clients are not allowed in the wireless network, then it is strongly recommended to disable the data rates below 12 Mbps. This will eliminate the need to send CTS frames for 802.11g protection as 802.11b clients can not detect these OFDM frames.

When 802.11b clients exist in the wireless network, then an 802.11b rate must be enabled and only an 802.11b rate can be configured as a mandatory / basic rate. In this case, is suggested to enable the data rates 11 Mbps and higher.

The recommended data rate configurations are the following:

802.11 Mode	Mandatory (Basic) Data Rates	Supported (Optional) Data Rates	Disabled Data Rates
802.11a /n	12 Mbps	18-54 Mbps, MCS 1 - MCS 7 (MCS 8 - MCS 15)	6, 9 Mbps, MCS 0
802.11g/n	12 Mbps	18-54 Mbps, MCS 1 - MCS 7 (MCS 8 - MCS 15)	1, 2, 5.5, 6, 9, 11 Mbps, MCS 0
802.11b/g/n	11 Mbps	12-54 Mbps, MCS 1 - MCS 7 (MCS 8 - MCS 15)	1, 2, 5.5, 6, 9 Mbps, MCS 0
802.11a	12 Mbps	18-54 Mbps	6, 9 Mbps
802.11g	12 Mbps	18-54 Mbps	6, 9 Mbps
802.11b/g	11 Mbps	12-54 Mbps	1, 2, 5.5, 6, 9 Mbps
802.11b	11 Mbps	None	1, 2, 5.5 Mbps

For a voice only application, data rates higher than 24 Mbps (36, 48 and 54 Mbps) can optionally be enabled or disabled, but there is no advantage from a capacity or throughput perspective and enabling these rates could potentially increase the number of retries for a data frame.

If deploying in an environment where excessive retries may be a concern, then a limited set of the data rates can be used (e.g. 12, 24, 54, MCS 1, MCS 4, MCS 7), where the lowest enabled rate is the mandatory / basic rate.

For rugged environments or deployments requiring maximum range, it is recommended to enable 6 Mbps as a mandatory / basic rate.

To preserve high capacity and throughput, data rates of 24 Mbps and higher only can be enabled (24-54 Mbps, MCS 3 - MCS 7).

If using other applications like video or virtual desktop, then it is recommended to enable these higher data rates including 802.11n rates (MCS 1 - MCS 15).

Note: Some environments may require that a lower data rate be enabled due to use of legacy clients, environmental factors or maximum range is required.

Set only the lowest data rate enabled as the single mandatory / basic rate. Multicast packets will be sent at the highest mandatory / basic data rate enabled.

Note that capacity and throughput are reduced when lower rates are enabled.

Call Capacity

Design the network to accommodate the desired call capacity.

The Cisco Access Point can support up to 27 bi-directional voice streams for both 802.11a/n and 802.11g/n at a data rate of 24 Mbps or higher. To achieve this capacity, there must be minimal wireless LAN background traffic and radio frequency (RF) utilization.

The number of calls may vary depending on the data rate, initial channel utilization, and the environment.

Max # of Streams	Audio Codec	Audio Bit Rate	802.11 Mode	Data Rate
13	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	6 Mbps
20	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	12 Mbps
27	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	24 Mbps or higher

When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced to the following:

Max # of Streams	Audio Codec	Audio Bit Rate	802.11 Mode	Data Rate
5	G.722 / G.711	64 Kbps	802.11a/n or 802.11g/n + Bluetooth Disabled	12-54 Mbps, MCS 1 - MCS 7

Note: It is highly recommended to use 802.11a/n if using Bluetooth.

Video Calls

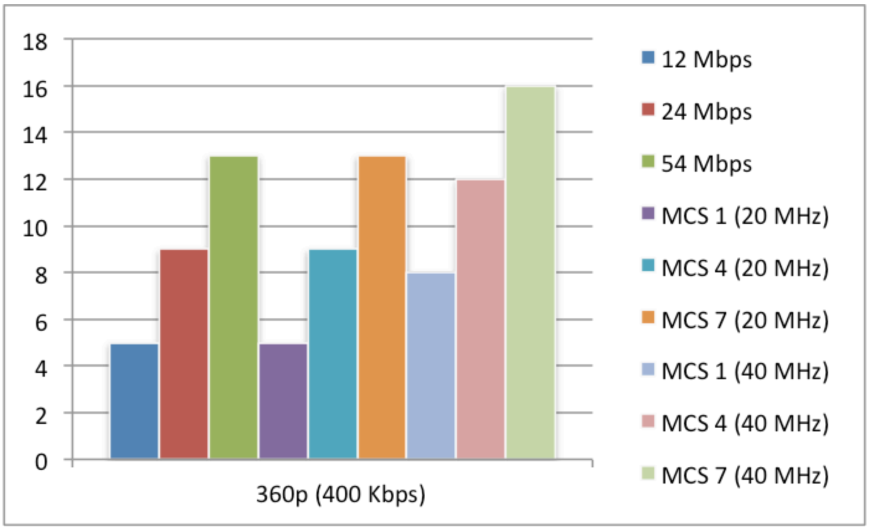
Video calls over Wireless LAN will significantly reduce the potential call capacity.

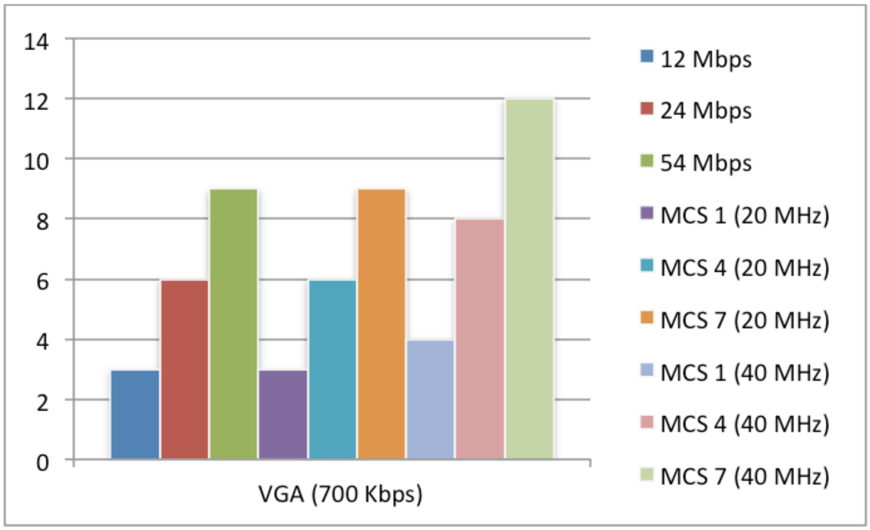
Below lists the maximum number of video calls (single bi-directional voice and video stream) supported per access point / channel for each video bit rate.

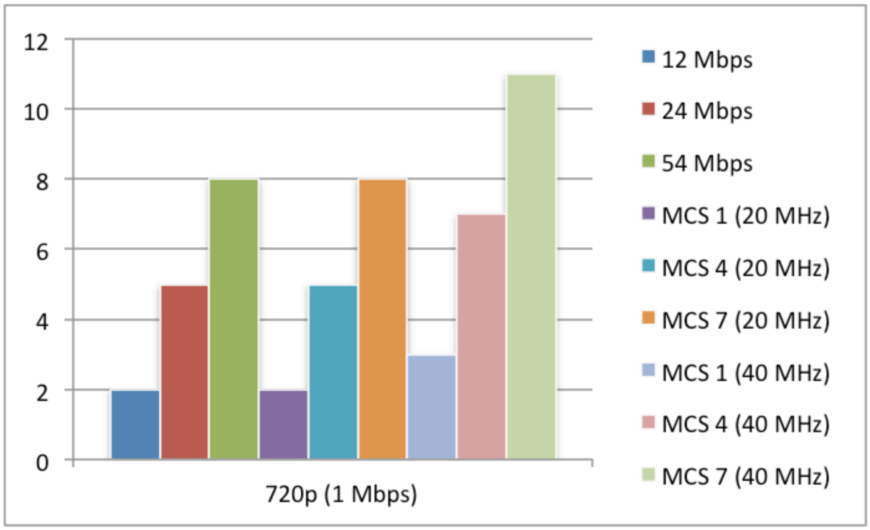
If there are two Cisco Cius communicating to each other, then that is two bi-directional voice and video streams.

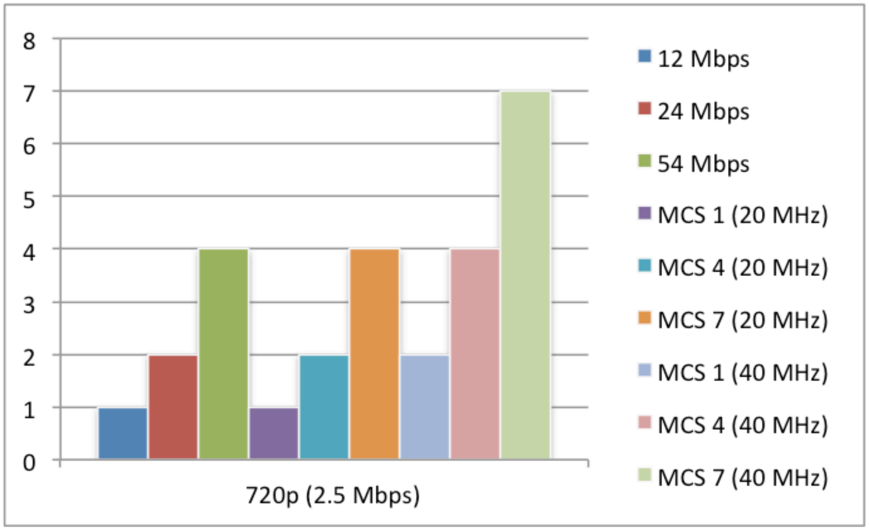
Max # of Video Calls	802.11 Mode	802.11 Data Rate	Audio Codec	Audio Bit Rate	Video Type	Video Resolution	Video Bit Rate
5-13	802.11a/n or 802.11g/n+ Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps
5-13	802.11a/n or 802.11g/n+ Bluetooth	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps

	Disabled						
8-16	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	360p	640 x 360	400 Kbps
3-9	802.11a/n or 802.11g/n+ Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps
3-9	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps
4-12	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	VGA	640 x 480	700 Kbps
2-8	802.11a/n or 802.11g/n+ Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
2-8	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
3-11	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	1000 Kbps
1-4	802.11a/n or 802.11g/n+ Bluetooth Disabled	12-54 Mbps	G.722 / G.711	64 Kbps	720p	1280 x 720	2500 Kbps
1-4	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (20 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	2500 Kbps
2-7	802.11a/n or 802.11g/n+ Bluetooth Disabled	MCS 1 - MCS 7 (40 MHz Channels)	G.722 / G.711	64 Kbps	720p	1280 x 720	2500 Kbps


18
16
14
12
10
8
6
4
2
0
360p (400 Kbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)


14
12
10
8
6
4
2
0
VGA (700 Kbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)


12
10
8
6
4
2
0
720p (1 Mbps)
12 Mbps
24 Mbps
54 Mbps
MCS 1 (20 MHz)
MCS 4 (20 MHz)
MCS 7 (20 MHz)
MCS 1 (40 MHz)
MCS 4 (40 MHz)
MCS 7 (40 MHz)



Note: Currently there is no Call Admission Control support for video.

Dynamic Transmit Power Control (DTPC)

To ensure packets are exchanged successfully between Cisco Cius and the access point, Dynamic Transmit Power Control (DTPC) should be enabled.

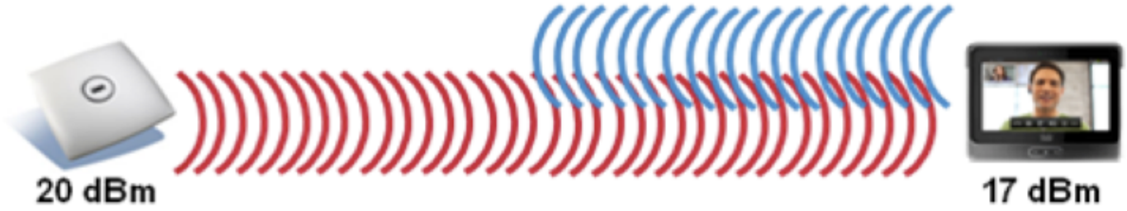
DTPC prevents one-way audio when RF traffic is heard in one direction only.

If the access point does not support DTPC, then Cisco Cius will use the highest available transmit power depending on the current channel and data rate.

When using an access point that supports DTPC, set the client power to match the local access point power.

Do not use default setting of **Max** power for client power on Cisco Autonomous Access Points as that will not advertise DTPC to the client.

The access point's radio transmit power should not have a transmit power greater than what Cisco Cius can support.



Rugged Environments

When deploying Cisco Cius in a rugged environment (e.g. manufacturing, warehouse, retail), additional tuning on top of the standard design recommendations may be necessary.

Below are the key items to focus on when deploying a wireless LAN in a rugged environment.

Access Point and Antenna Selection

For rugged environments, it is recommended to select an access point platform that requires external antennas (e.g. Cisco 1602e, 2602e, 3502e, 3602e Series Access Points). It is also important to ensure an antenna type is selected which can operate well in rugged environments.

Access Point Placement

It is crucial that line of sight to the access point's antennas is maximized by minimizing any obstructions between Cisco Cius and the access point. Ensure that the access point and/or antennas are not mounted behind any obstruction or on or near a metal or glass surface.
If access points with integrated antennas (e.g. Cisco 1040, 1130, 1140, 1602i, 2602i, 3502i and 3602i Series Access Points) are to be used in some areas, then it is recommended to mount those access points on the ceiling as they have omni-directional antennas and are not designed to be patches.

Frequency Band

As always, it is recommended to use 5 GHz. Use of 2.4 GHz, especially when 802.11b rates are enabled, may not work well.
For the 5 GHz channel set, it is recommended to use a 8 or 12 channel plan only; disable UNII-2 extended channels if possible.

Data Rates

The standard recommended data rate set of 12-54 Mbs may not work well if multipath is present at an elevated level. Therefore, it is recommended to enable lower data rates (e.g. 6 Mbps) to operate better in such an environment.
If 5 GHz is used for VoWLAN only, then it is also recommended to disable data rates above 24 Mbps (i.e. 36, 48, 54 Mbps) to increase first transmission success (e.g. 6 as mandatory, 12 and 24 as supported). If 5 GHz is also used for data, video or other applications, then is suggested to keep the higher data rates enabled (e.g. 6 as mandatory, 9, 12-54 as supported).

Transmit Power

Due to the potential of elevated multipath in rugged environments, the transmit power of the access point and Cisco Cius should also be restricted. This is more important if planning to deploy 2.4 GHz in a rugged environment.
If using auto transmit power, the access point transmit power can be configured to use a specified range (maximum and minimum power levels) to prevent the access point from transmitting too hot as well as too weak (e.g. 5 GHz maximum of 16 dBm and minimum of 11 dBm).
Cisco Cius will utilize the access point's current transmit power setting to determine what transmit power it uses for transmitted frames when DTPC is enabled in the access point's configuration.

Fast Roaming

It is recommended to utilize CCKM for fast roaming. Enabling CCKM also reduces the number of frames in the handshake when roaming to only two frames. Reducing the number of frames during a roam, increases the chances of roam success.
When using 802.1x authentication, it is important to use the recommended EAPOL key settings. See the **WLAN Controller Advanced EAP Settings** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

Quality of Service (QoS)

Need to ensure that DSCP values are preserved throughout the wired network, so that Cisco Unified Wireless LAN Controller and access points can set the WMM UP tag for voice and call control frames correctly.

Beamforming

If using Cisco 802.11n access points, then Beamforming (ClientLink) should be enabled, which can help with client reception.
See the **Beamforming (ClientLink)** section in **Configuring the Cisco Unified Wireless LAN Controller and Access Points** for more information.

Multipath

Multipath occurs when RF signals take multiple paths from a source to a destination.

A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination, which creates signal energy loss.

When the different waveforms combine, they cause distortion and affect the decoding capability of the receiver, as the signal quality is poor.

Multipath can exist in environments where there are reflective surfaces (e.g. metal, glass, etc.). Avoid mounting access points on these surfaces.

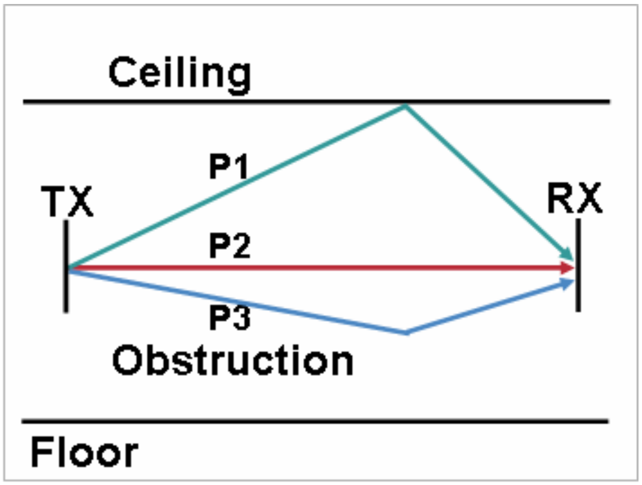
Below is a list of multipath effects:

Data Corruption
Occurs when multipath is so severe that the receiver is unable to detect the transmitted information.

Signal Nulling
Occurs when the reflected waves arrive exactly out of phase with the main signal and cancel the main signal completely.

Increased Signal Amplitude
Occurs when the reflected waves arrive in phase with the main signal and add on to the main signal thereby increasing the signal strength.

Decreased Signal Amplitude
Occurs when the reflected waves arrive out of phase to some extent with the main signal thereby reducing the signal amplitude.



Use of Orthogonal Frequency Division Multiplexing (OFDM), which is used by 802.11a and 802.11g, can help to reduce issues seen in high multipath environments.

If using 802.11b in a high multipath environment, lower data rates should be used in those areas (e.g. 1 and 2 Mbps).

Use of antenna diversity can also help in such environments.

Verification with Site Survey Tools

These are many tools and applications that can be utilized to verify coverage, quality and configuration.

- Cisco Prime Network Control System (NCS) for Unified Wireless LAN Management http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps11682/ps11686/ps11688/data_sheet_c78-650051.html

- Cisco Wireless Control System (WCS) for Unified Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

- Cisco Wireless LAN Solution Engine (WLSE) for Cisco Autonomous Wireless LAN Management

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6380/ps6563/ps3915/ps6839/product_data_sheet0900aecd80410b92.html

- Cisco Spectrum Expert

  http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html

- Cisco Unified Operations Manager

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/data_sheet_c78-636705.html

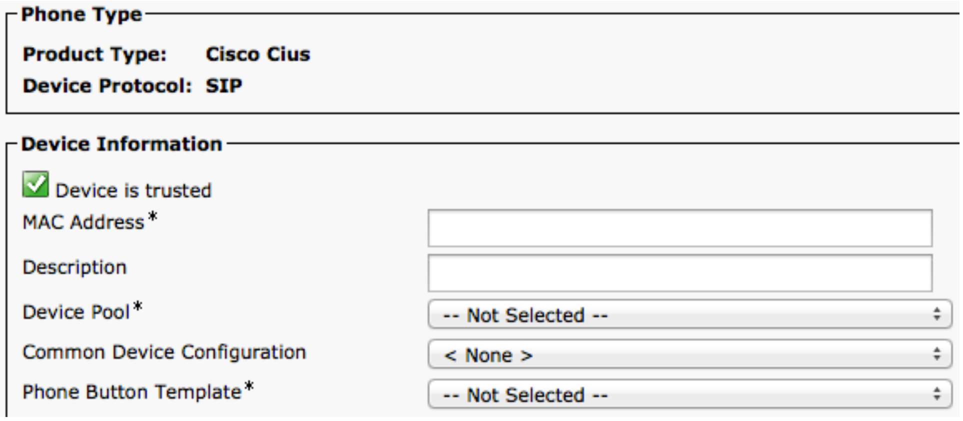
- AirMagnet (Survey, WiFi Analyzer, VoFi Analyzer, Spectrum Analyzer)

  http://www.airmagnet.com

Configuring Cisco Unified Communications Manager

Cisco Unified Communications Manager offers many different product, call and security features.

When adding Cisco Cius to the Cisco Unified Communications Manager it must be provisioned using the Ethernet MAC address as the Wireless LAN MAC is used for Wi-Fi connectivity only.



Phone Type

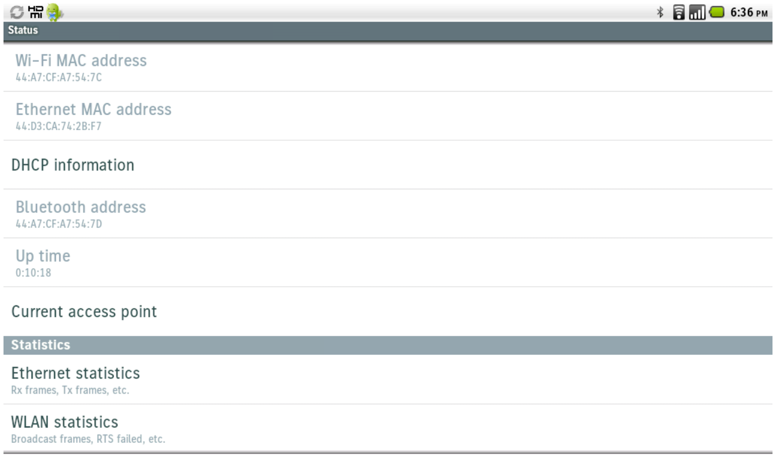
Product Type:	**Cisco Cius**
Device Protocol:	**SIP**

Device Information

☑ Device is trusted

MAC Address*	
Description	
Device Pool*	-- Not Selected --
Common Device Configuration	< None >
Phone Button Template*	-- Not Selected --

The Ethernet MAC address can be found by navigating to **Settings > About Device > Status** on Cisco Cius.



Status

Wi-Fi MAC address
44:A7:CF:A7:54:7C

Ethernet MAC address
44:D3:CA:74:2B:F7

DHCP information

Bluetooth address
44:A7:CF:A7:54:7D

Up time
0:10:18

Current access point

Statistics

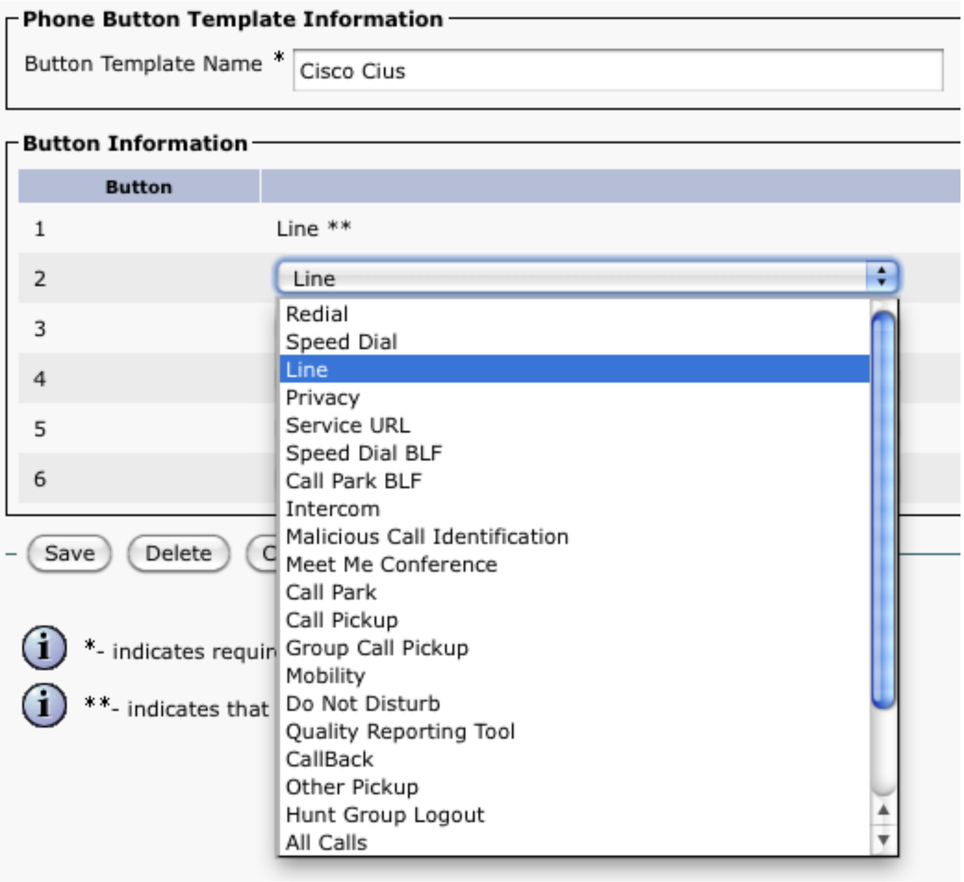
Ethernet statistics
Rx frames, Tx frames, etc.

WLAN statistics
Broadcast frames, RTS failed, etc.

Phone Button Templates

Cisco Cius supports up to 6 lines. The default phone button template includes support for 2 lines and 4 speed dials.

Custom phone button templates can be created with the option for many different features, which can then be applied on a device or group level.



Phone Button Template Information

Button Template Name * Cisco Cius

Button Information

Button	
1	Line **
2	Line
3	
4	
5	
6	

*- indicates requir

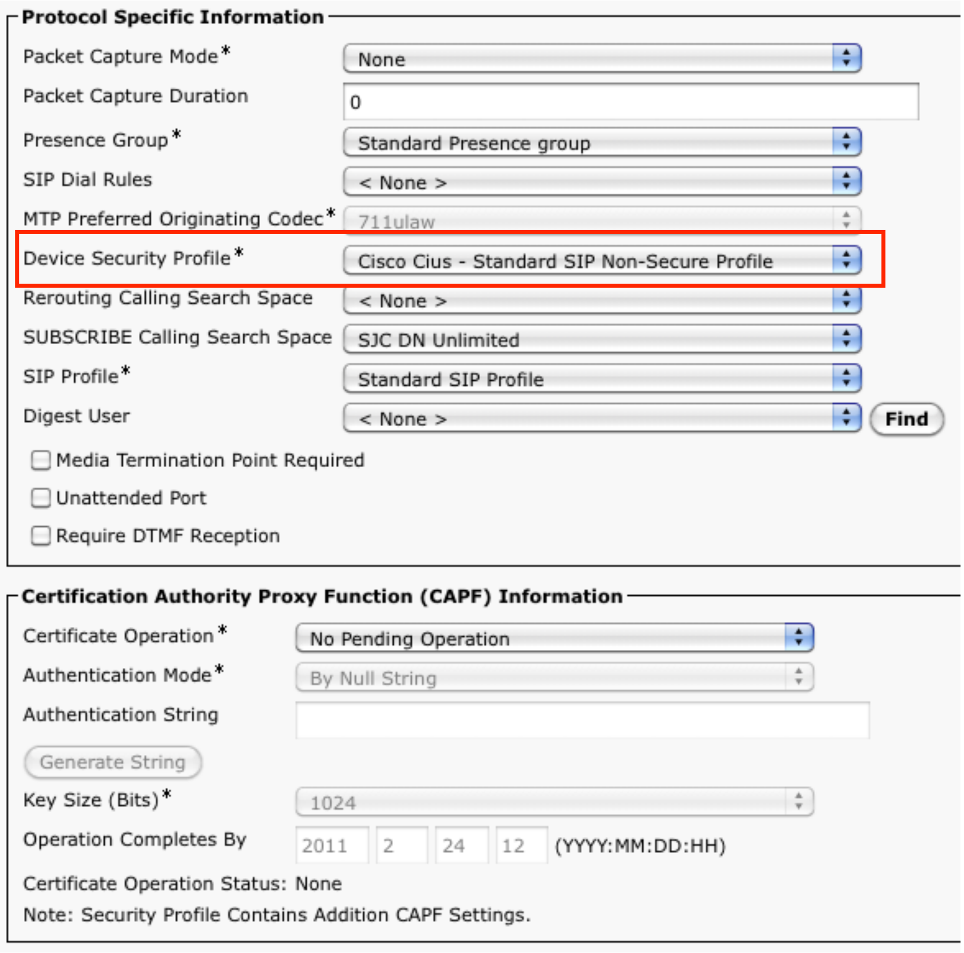
**- indicates that

Security Profiles

Security profiles can be utilized to enable authenticated mode or encrypted mode, where signaling, media and configuration file encryption is then enabled.

The Certificate Authority Proxy Function (CAPF) must be operational in order to utilize a Locally Signed Certificate (LSC) with a security profile.

Cisco Cius has a Manufactured Installed Certificate (MIC), which can be utilized with a security profile as well.



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Cius - Standard SIP Non-Secure Profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	SJC DN Unlimited
SIP Profile*	Standard SIP Profile
Digest User	< None >

□ Media Termination Point Required
□ Unattended Port
□ Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication String	
Key Size (Bits)*	1024
Operation Completes By	2011 2 24 12 (YYYY:MM:DD:HH)

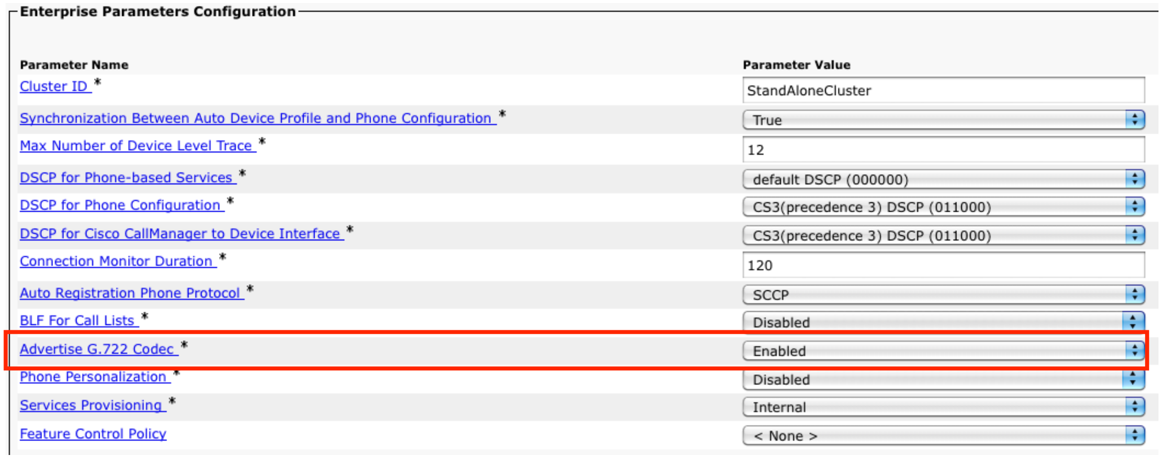
Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

G.722 Advertisement

Cisco Unified Communications Manager supports the ability to configure whether G.722 is to be a supported codec system wide or not.

G.722 and iSAC codecs can be disabled at the enterprise phone, common phone profile or individual phone level by setting **Advertise G.722 and iSAC Codecs** to disabled.



Enterprise Parameters Configuration

Parameter Name	Parameter Value
Cluster ID *	StandAloneCluster
Synchronization Between Auto Device Profile and Phone Configuration *	True
Max Number of Device Level Trace *	12
DSCP for Phone-based Services *	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120
Auto Registration Phone Protocol *	SCCP
BLF For Call Lists *	Disabled
Advertise G.722 Codec *	Enabled
Phone Personalization *	Disabled
Services Provisioning *	Internal
Feature Control Policy	< None >

For more information, refer to the Cisco Unified Communications Manager documentation.

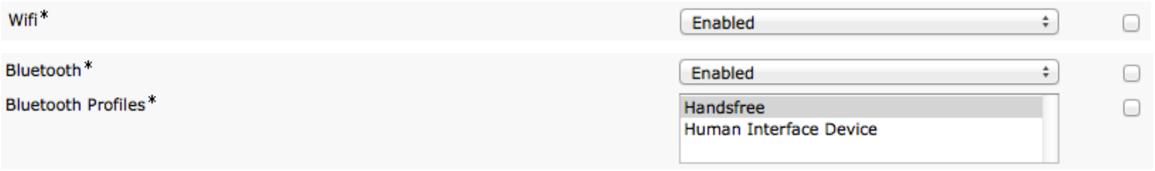
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Common Settings

Some settings such as Wireless LAN and Bluetooth can be configured on an enterprise phone, common phone profile or individual phone level.

Wireless LAN and Bluetooth are enabled by default.

Override common settings can be enabled at either configuration level.



Wifi *	Enabled	☐
Bluetooth *	Enabled	☐
Bluetooth Profiles *	Handsfree Human Interface Device	☐

Audio and Video Bit Rates

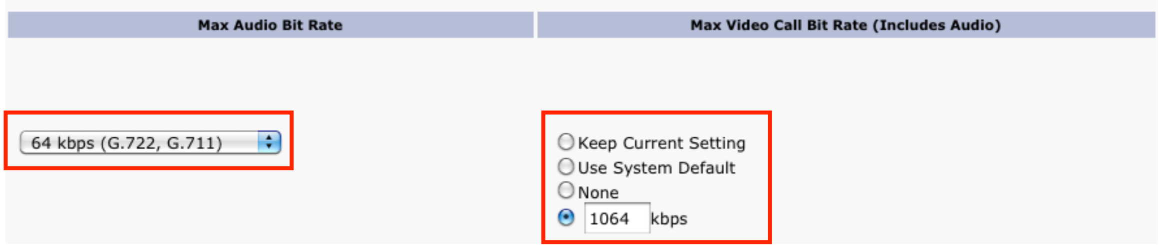
The audio and video bit rate can be configured by creating or editing existing Regions in the Cisco Unified Communications Manager.

It is recommended to select G.722 or G.711 for the audio codec.

By default the video call bit rate is set to 384 Kbps.

For typical deployments, it is recommended to utilize the 360p bit rate (400-499 Kbps) for the video stream.

For enhanced video quality, set the video call bit rate to at least 1 Mbps to utilize 720p (total 1064 Kbps including G.722 audio).



Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)
64 kbps (G.722, G.711)	○ Keep Current Setting ○ Use System Default ○ None ● 1064 kbps

Use the following information to configure the audio bit rate to be used for audio or audio + video calls.

Audio Codec	Audio Bit Rate
G.722 / G.711	64 Kbps
iSAC	32 Kbps
iLBC	16 Kbps
G.729	8 Kbps
AAC-LD	256 Kbps

Use the following information to configure the video bit rate to be used for video calls.

The value configured will determine the resolution of the transmitted video stream from Cisco Cius.

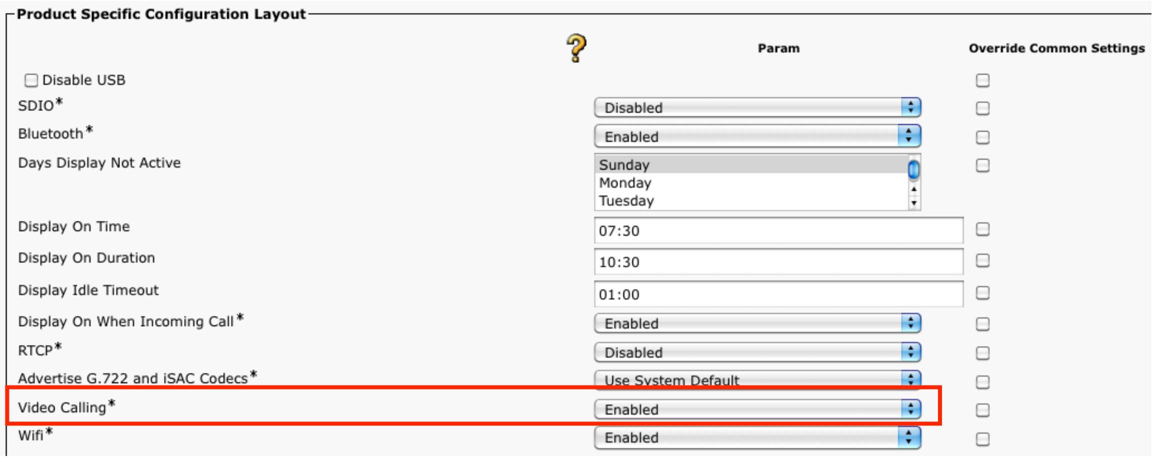
Cisco Cius will be able to receive up to 720p video depending on the remote device's capabilities, where the region settings configuration is factored in.

Video Type	Video Resolution	Frames per Second (fps)	Video Bit Rate Range
QCIF	176 x 144	30	17-249 Kbps
CIF	352 x 288	30	250-399 Kbps
360p	640 x 360	30	400-499 Kbps
VGA	640 x 480	30	500-999 Kbps
720p	1280 x 720	30	1000-2500 Kbps

Video Calling Capabilities

In order for Cisco Cius to send and receive video, that capability must be enabled in the Cisco Unified Communications Manager.

Set the **Video Calling** option to **Enabled** in the configuration within the Product Specific Configuration Layout section.

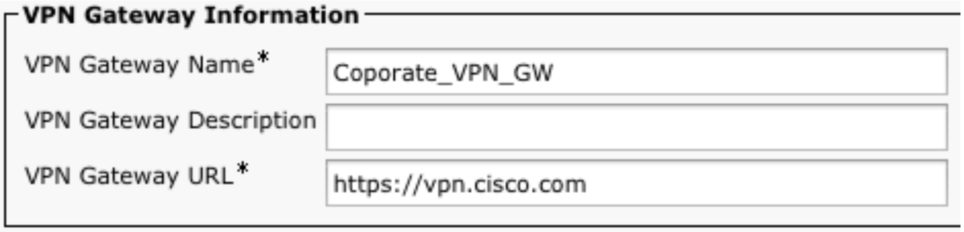


Product Specific Configuration Layout

	Param	Override Common Settings
□ Disable USB		□
SDIO*	Disabled	□
Bluetooth*	Enabled	□
Days Display Not Active	Sunday Monday Tuesday	□
Display On Time	07:30	□
Display On Duration	10:30	□
Display Idle Timeout	01:00	□
Display On When Incoming Call*	Enabled	□
RTCP*	Disabled	□
Advertise G.722 and iSAC Codecs*	Use System Default	□
Video Calling*	Enabled	□
Wifi*	Enabled	□

VPN Configuration

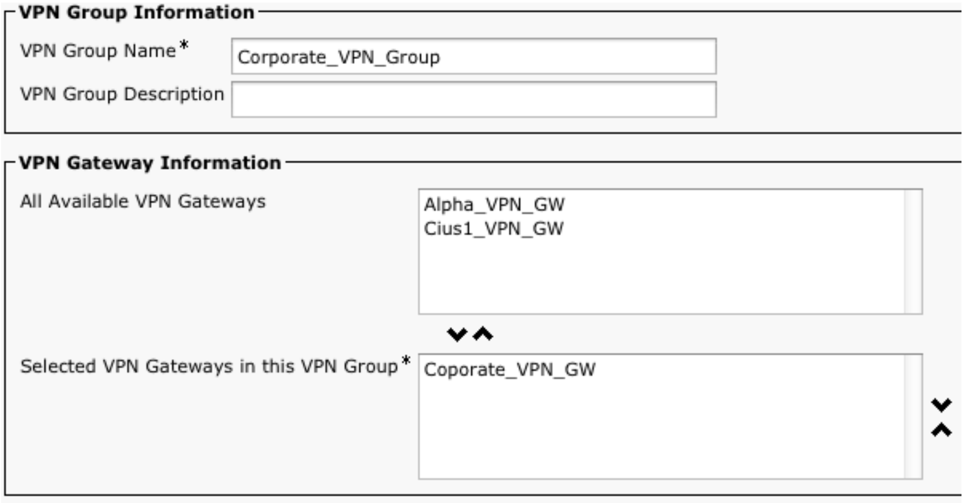
VPN configuration information can be pushed down from the administrator via Cisco Unified Communications Manager. A VPN gateway must be created, where the name and VPN gateway URL are defined.



VPN Gateway Information

VPN Gateway Name*	Coporate_VPN_GW
VPN Gateway Description	
VPN Gateway URL*	https://vpn.cisco.com

A VPN group must also be created, which contains information about which VPN gateway will be utilized.



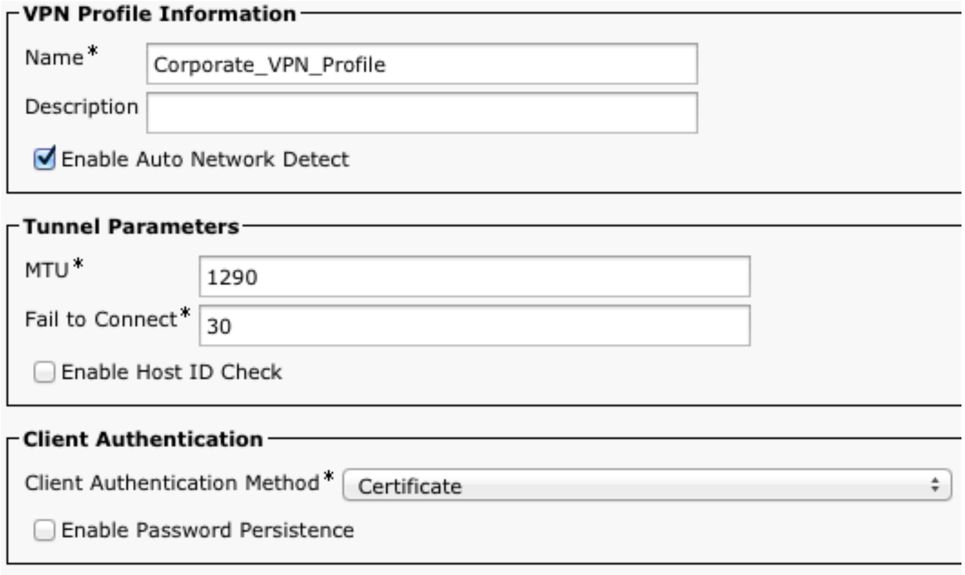
VPN Group Information

VPN Group Name*	Corporate_VPN_Group
VPN Group Description	

VPN Gateway Information

All Available VPN Gateways	Alpha_VPN_GW Cius1_VPN_GW
Selected VPN Gateways in this VPN Group*	Coporate_VPN_GW

A VPN profile must be configured, which specifies which type of client authentication will be utilized as well as other parameters.



VPN Profile Information

Name* Corporate_VPN_Profile

Description

☑ Enable Auto Network Detect

Tunnel Parameters

MTU* 1290

Fail to Connect* 30

□ Enable Host ID Check

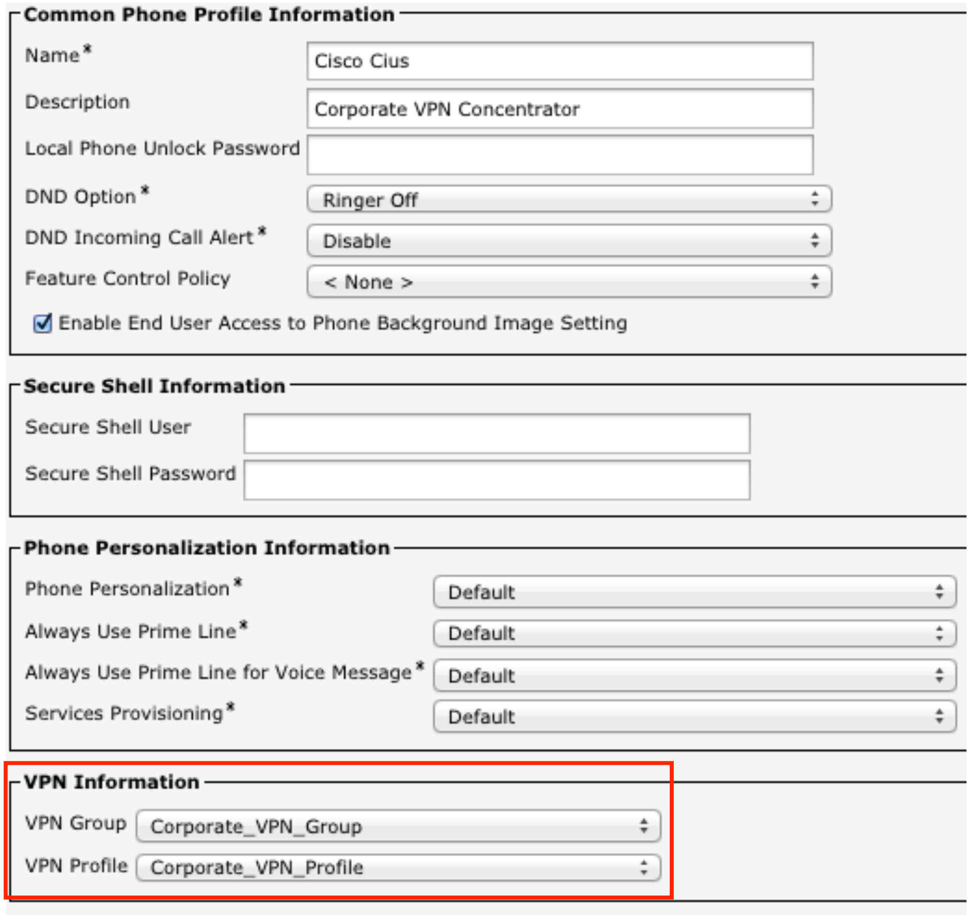
Client Authentication

Client Authentication Method* Certificate

□ Enable Password Persistence

Once the VPN group and profile have been configured, they can then be applied to a Common Phone Profile, which in turn can be applied to a specific device.

If Cisco Cius is currently connected to a mobile network or any other type of network and is unable to connect to the Cisco Unified Communications Manager then it can attempt to establish a VPN session automatically if a VPN profile is configured.



Common Phone Profile Information

Name* Cisco Cius

Description Corporate VPN Concentrator

Local Phone Unlock Password

DND Option* Ringer Off

DND Incoming Call Alert* Disable

Feature Control Policy < None >

☑ Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User

Secure Shell Password

Phone Personalization Information

Phone Personalization* Default

Always Use Prime Line* Default

Always Use Prime Line for Voice Message* Default

Services Provisioning* Default

VPN Information

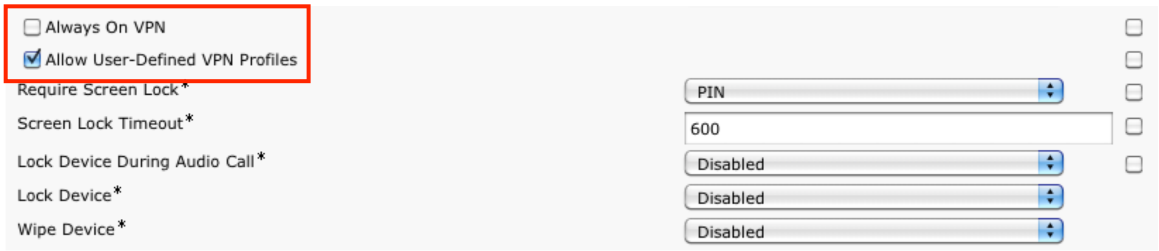
VPN Group Corporate_VPN_Group

VPN Profile Corporate_VPN_Profile

Always on VPN and **Allow User-Defined VPN Profiles** can be configured on an enterprise phone, common phone profile or individual phone configuration level.

Always On VPN can help ensure that Cisco Cius remains on a secure network and is always connected to Cisco Unified Communications Manager.

Allow User-Defined VPN Profiles can enable the user to create their own VPN profiles.



☐ Always On VPN		☐
☑ Allow User-Defined VPN Profiles		☐
Require Screen Lock*	PIN	☐
Screen Lock Timeout*	600	☐
Lock Device During Audio Call*	Disabled	☐
Lock Device*	Disabled	
Wipe Device*	Disabled	

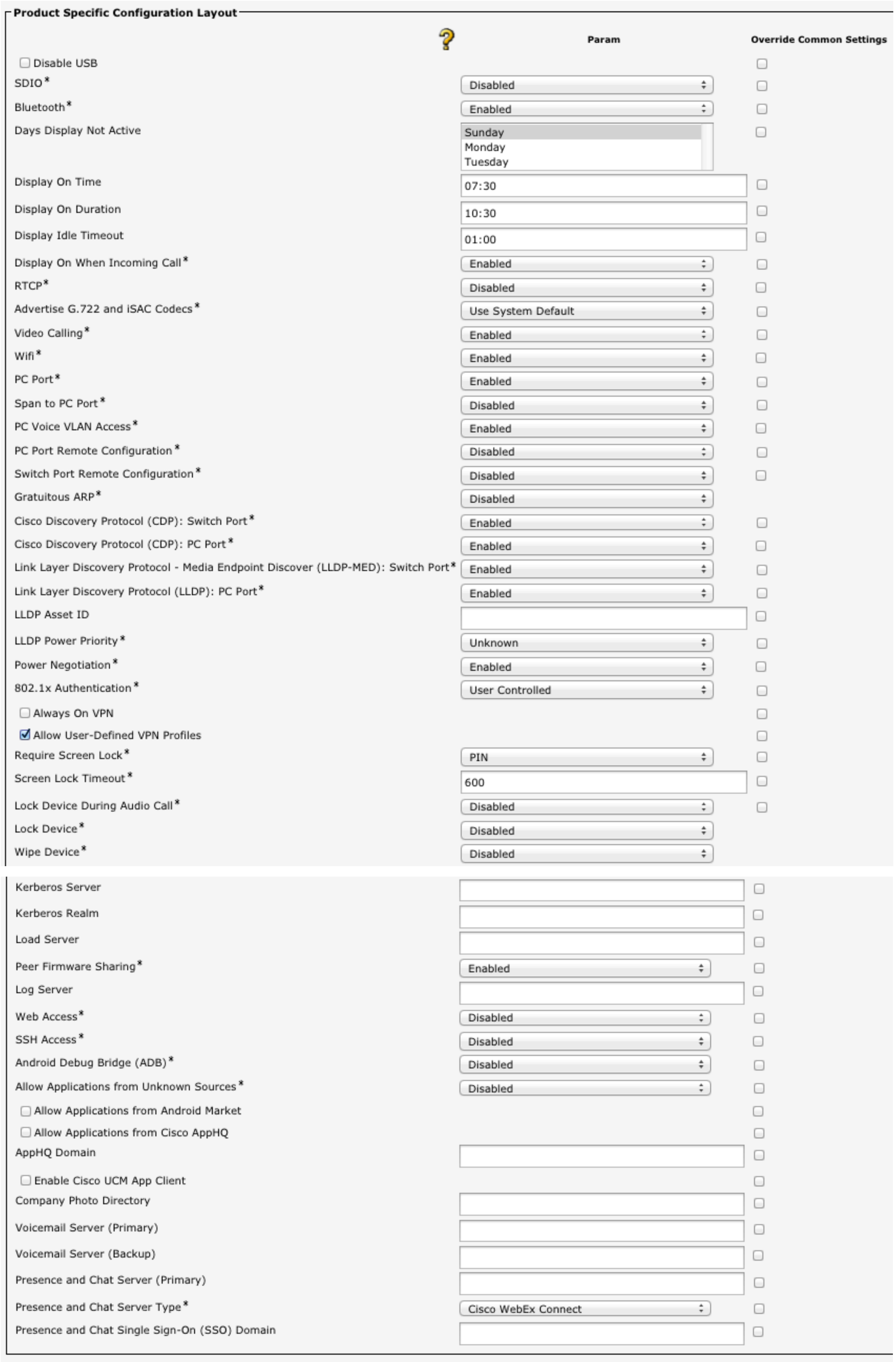
Product Specific Configuration Options

In Cisco Unified Communications Manager Administration, the following Cisco Cius configuration options are available.

For a description of these options, click **?** at the top of the configuration page.

Product specific configuration options can be configured in bulk via the Bulk Admin Tool if using Cisco Unified Communications Manager.

Some of the product specific configuration options can be configured on an enterprise phone, common phone profile or individual phone configuration level.



Product Specific Configuration Layout

	Param	Override Common Settings
□ Disable USB		□
SDIO*	Disabled	□
Bluetooth*	Enabled	□
Days Display Not Active	Sunday Monday Tuesday	□
Display On Time	07:30	□
Display On Duration	10:30	□
Display Idle Timeout	01:00	□
Display On When Incoming Call*	Enabled	□
RTCP*	Disabled	□
Advertise G.722 and iSAC Codecs*	Use System Default	□
Video Calling*	Enabled	□
Wifi*	Enabled	□
PC Port*	Enabled	□
Span to PC Port*	Disabled	□
PC Voice VLAN Access*	Enabled	□
PC Port Remote Configuration*	Disabled	□
Switch Port Remote Configuration*	Disabled	□
Gratuitous ARP*	Disabled	
Cisco Discovery Protocol (CDP): Switch Port*	Enabled	□
Cisco Discovery Protocol (CDP): PC Port*	Enabled	□
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled	□
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled	□
LLDP Asset ID		□
LLDP Power Priority*	Unknown	□
Power Negotiation*	Enabled	□
802.1x Authentication*	User Controlled	□
□ Always On VPN		□
☑ Allow User-Defined VPN Profiles		□
Require Screen Lock*	PIN	□
Screen Lock Timeout*	600	□
Lock Device During Audio Call*	Disabled	□
Lock Device*	Disabled	
Wipe Device*	Disabled	
Kerberos Server		□
Kerberos Realm		□
Load Server		□
Peer Firmware Sharing*	Enabled	□
Log Server		□
Web Access*	Disabled	□
SSH Access*	Disabled	□
Android Debug Bridge (ADB)*	Disabled	□
Allow Applications from Unknown Sources*	Disabled	□
□ Allow Applications from Android Market		□
□ Allow Applications from Cisco AppHQ		□
AppHQ Domain		□
□ Enable Cisco UCM App Client		□
Company Photo Directory		□
Voicemail Server (Primary)		□
Voicemail Server (Backup)		□
Presence and Chat Server (Primary)		□
Presence and Chat Server Type*	Cisco WebEx Connect	□
Presence and Chat Single Sign-On (SSO) Domain		□

Field Name	**Description**
Disable USB	Disable the USB ports on the device and dock.
SDIO	Indicates whether the SDIO device on the device is enabled or disabled.
Bluetooth	Indicates whether the Bluetooth device on the device is enabled or disabled.
Days Display Not Active	This field allows the user to specify the days that the backlight is to remain off by default. Typically this would be Saturday and Sunday for US corporate customers. Saturday and Sunday should be the default. The list contains all of the days of the week. To turn off backlight on Saturday and Sunday the User would hold down Control and select Saturday and Sunday.
Display On Time	This field indicates the time of day the display is to automatically turn itself on for days listed in the off schedule. The value should be in a 24 hour format. Where 0:00 is the beginning of the day and 23:59 is the end of the day. Leaving this field blank will activate the display at the default time of the day (e.g. - "7:30"). To set the display to turn on at 7:00AM the user would enter "07:00" without the quotes. If they wanted the display to turn on at 2:00PM they would enter "14:00" without the quotes.
Display On Duration	This field indicates the amount of time the display is to be active for when it is turned on by the programmed schedule. Leaving this field blank will make the phone use a pre-determined default value of "10:30". Maximum value is 24 hours. This value is in free form hours and minutes. "1:30" would activate the display for one hour and 30 minutes.
Display Idle Timeout	This field indicates how long to wait before the display is turned off when it was turned on by user activity. This inactivity timer will continually reset itself during user activity. Leaving this field blank will make the device use a pre-determined default value of one hour. Maximum value is 24 hours. This value can be in free form hours and minutes. "1:30" would turn off the display after one hour and 30 minutes of inactivity.
Display On When Incoming Call	When the device is in screen saver mode, this will turn the display on when a call is ringing.
RTCP	Maintains statistic for audio.
Advertise G.722 and iSAC Codecs	Indicates whether the phone application will advertise the wideband codecs to the Cisco Unified Communications Manager. Codec negotiation involves two steps: first, the phone application must advertise the supported codec(s) to the Cisco Unified Communications Manager (not all endpoints support the same set of codecs). Second, when the Cisco Unified Communications Manager gets the list of supported codecs from all phones involved in the call attempt, it chooses a commonly-supported codec based on various factors, including the region pair setting. Valid values specify Use System Default (this phone application will defer to the setting specified in the enterprise parameter, Advertise G.722 Codec), Disabled (this phone application will not advertise the wideband codecs to the Cisco Unified Communications Manager) or Enabled (this phone application will advertise the wideband codecs to the Cisco Unified Communications Manager).
Video Calling	When enabled, indicates that the device will participate in video calls.
Wifi	Indicates whether the Wi-Fi on the device is enabled or disabled.
PC Port	Indicates whether the PC port on the dock is enabled or disabled. The port labeled

	"COMPUTER" on the back of the dock connects a PC or workstation to the dock so they can share a single network connection.
Span to PC Port	Indicates whether the device will forward packets transmitted and received on the dock's network port to the PC port. Select Enabled if an application is being run on the PC port that requires monitoring of the device's traffic such as monitoring and recording applications (common in call center environments) or network packet capture tools used for diagnostic purposes. To use this feature PC Voice VLAN access must be enabled.
PC Voice VLAN Access	Indicates whether a device attached to the PC port on the dock is allowed access to the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the device. Set this setting to Enabled if an application is being run on the PC that requires monitoring of the device traffic. These could include monitoring and recording applications and use of network monitoring software for analysis purposes.
PC Port Remote Configuration	Allows remote configuration of the PC port speed and duplex of the device when docked. This overrides any manual configuration on the device.
Switch Port Remote Configuration	Allows remote configuration of the switch port speed and duplex of the device when docked. This overrides any manual configuration on the device. Be aware that configuring this port may cause the device to lose network connectivity when it is on the dock.
Gratuitous ARP	Indicates whether the device will learn MAC addresses from Gratuitous ARP responses. Disabling the device ability to accept Gratuitous ARP will prevent applications which use this mechanism for monitoring and recording of voice streams from working. If monitoring capability is not desired, change this setting to Disabled.
Cisco Discover Protocol (CDP): Switch Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the dock's switch port.
Cisco Discover Protocol (CDP): PC Port	Allows administrator to enable or disable Cisco Discovery Protocol (CDP) on the dock's PC port.
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the dock's switch port.
Link Layer Discovery Protocol - (LLDP): PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the dock's PC port.
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol.
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol.
Power Negotiation	Allows administrator to enable or disable Power Negotiation. Enable the Power Negotiation feature when the dock is connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, then you should disable the Power Negotiation feature before you power up accessories over PoE. When the Power Negotiation feature is disabled, the dock can power up accessories up to 12.9W.
802.1x Authentication	Specifies the 802.1x authentication feature status.

Always On VPN	Indicates whether the device will always start the VPN AnyConnect client and establish a connection with the configured VPN profile from the Cisco Unified Communications Manager.
Allow User-Defined VPN Profiles	This parameter controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles.
Require Screen Lock	This parameter indicates whether screen lock is required on the device. If "User Controlled" is selected, the device will not prompt for a PIN or password. The "PIN" and "Password" options require the user to enter a password to unlock the screen. A "PIN" is a numeric password that is at least four digits long. A "Password" is an alphanumeric password, consisting of at least 4 alphanumeric characters, one of which must be a non-numeric number, and one must be a capital letter.
Screen Lock Timeout	Maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it.
Lock Device During Audio Call	When the device is in a charging state and an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded.
Lock Device	This parameter allows the administrator to lock the device to prevent unauthorized user access.
Wipe Device	This parameter allows the administrator to erase the user data and configuration on the device.
Kerberos Server	Authentication server for web proxy Kerberos.
Kerberos Realm	Realm for web proxy Kerberos.
Load Server	Indicates that the device will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. This option enables you to indicate a local server to be used for firmware upgrades, which can assist in reducing install times, particularly for upgrades over a WAN. Enter the hostname or the IP address (using standard IP addressing format) of the server. The indicated server must be running TFTP services and have the load file in the TFTP path. If the load file is not found, the load will not install. The device will not be redirected to the TFTP server. If this field is left blank, the device will use the designated TFTP server to obtain its load files and upgrades.
Peer Firmware Sharing	PPID. Enables or disables Peer to Peer image distribution in order to allow a single device in a subnet to retrieve an image firmware file then distribute it to its peers - thus reducing TFTP bandwidth and providing for a faster firmware upgrade time.
Log Server	Specifies an IP address and port of a remote system where log messages are sent.
Web Access	This parameter indicates whether the device will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the device will block access to the device's internal web pages. These pages provide statistics and configuration information. Features, such as QRT (Quality Report Tool), will not function properly without access to the device's web pages. This setting will also affect any serviceability application such as CiscoWorks 2000 that relies on web access.

SSH Access	This parameter indicates whether the device will accept SSH connections. Disabling the SSH server functionality of the device will block access to the device.
Android Debug Bridge (ADB)	This parameter enables or disables the Android Debug Bridge (ADB) on the device.
Allow Applications from Unknown Sources	This parameter controls whether the user can install Android applications on the device from a URL or from Android packages (APK) that are received through email, instant message (IM), or from a Secure Digital (SD) card.
Allow Applications from Android Market	This parameter controls whether the user can install Android applications from the Google's Android Market.
Allow Applications from Cisco AppHQ	This parameter controls whether the user can install Android applications from the Cisco AppHQ.
AppHQ Domain	The fully-qualified domain name to use when users log into AppHQ. If empty, the user will specify their own domain name along with their username. The AppHQ domain is used to associate the user to a given Custom AppHQ store, if it exists. Example: cisco.com.
Enable Cisco UCM App Client	This parameter controls whether the Application Client runs on the device. When the Application Client is enabled, users can select the applications they would like to install from the Cisco Unified Communications Manager.
Company Photo Directory	This parameter specifies the URL which the device can query for a user and get the image associated with that user.
Voicemail Server (Primary)	Hostname or IP address of the primary visual voicemail server.
Voicemail Server (Backup)	Hostname or IP address of the backup visual voicemail server.
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server.
Presence and Chat Server Type	This parameter indicates the type of server specified in the "Presence and Chat Server" field.
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain used by Cisco WebEx Connect Cloud to perform Single-Sign-On (SSO) authentication against an enterprise.

For more information on these features, see the Cisco Cius Administration Guide or the Cisco Cius Release Notes.

http://www.cisco.com/en/US/products/ps11156/prod_maintenance_guides_list.html

http://www.cisco.com/en/US/products/ps11156/prod_release_notes_list.html

Configuring the Cisco Unified Wireless LAN Controller and Access Points

When configuring the Cisco Unified Wireless LAN Controller and Access Points, use the following guidelines:

- Ensure **CCKM** is **Enabled** if utilizing 802.1x authentication
- Set **Quality of Service (QoS)** to **Platinum**

- Set the **WMM Policy** to **Required**
- Ensure **Session Timeout** is enabled and configured correctly
- Ensure **Aironet IE** is **Enabled**
- Set **DTPC Support** to **Enabled**
- Disable **P2P (Peer to Peer) Blocking Action** / **Public Secure Packet Forwarding (PSPF)**
- Ensure **Client Exclusion** is configured correctly
- Disable **DHCP Address Assignment Required**
- Set **MFP Client Protection** to **Optional** or **Disabled**
- Set the **DTIM Period** to **2**
- Set **Client Load Balancing** to **Disabled**
- Set **Client Band Select** to **Disabled**
- Set **IGMP Snooping** to **Enabled**
- Enable **Symmetric Mobile Tunneling Mode** if Layer 3 mobility is utilized
- Enable **Short Preamble** if using 2.4 GHz
- Enable **ClientLink** if utilizing Cisco 802.11n Access Points
- Configure the **Data Rates** as necessary
- Enable **CCX Location Measurement**
- Configure **Auto RF** as necessary
- Set **Admission Control Mandatory** to **Enabled** for **Voice**
- Set **Load Based CAC** to **Enabled** for **Voice**
- Configure **SIP CAC Support** for **Voice** as necessary
- Enable **Traffic Stream Metrics** for **Voice**
- Set **Admission Control Mandatory** to **Disabled** for **Video**
- Set **EDCA Profile** to **Voice and Video Optimized**
- Set **Enable Low Latency MAC** to **Disabled**
- Ensure that **Power Constraint** is **Disabled**
- Enable **Channel Announcement** and **Channel Quiet Mode**
- Configure the **802.11n High Throughput Data Rates** as necessary
- Configure the **Frame Aggregation** settings
- Enable **CleanAir** if utilizing Cisco Access Points with CleanAir technology
- Configure **Multicast Direct Feature** as necessary
- Set the **802.1p tag** to **6** for the **Platinum** QoS profile

Note: If clients from other regions are present and will attempt to associate with the wireless LAN, then ensure that World Mode (802.11d) is enabled.

When using 802.1x authentication, it is recommended to implement CCKM to offer fast secure roaming.

SSID / WLAN Settings

It is recommended to have a separate SSID for Cisco Cius.

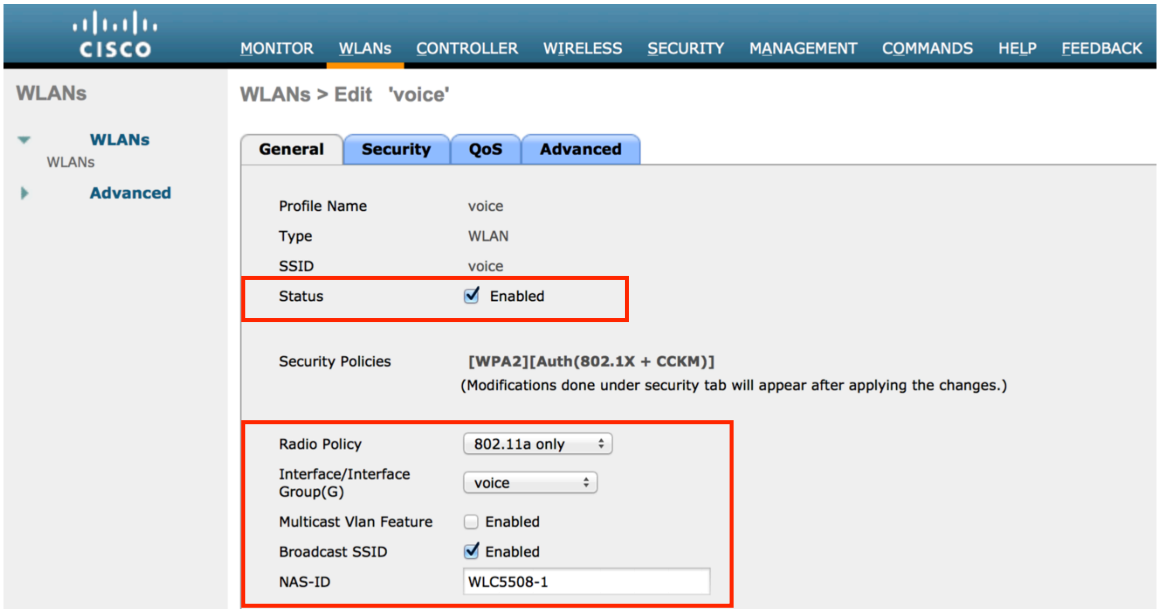
However, if there is an existing SSID configured to support voice and/or video capable Cisco Wireless LAN endpoints already, then that WLAN can be utilized instead.

The SSID to be used by Cisco Cius can be configured to only apply to a certain 802.11 radio type.

It is recommended to have Cisco Cius operate on the 5 GHz band due to have many channels available and not as many interferers as the 2.4 GHz band has.

Enabling **Broadcast SSID** can help with deployment of Cisco Cius where the network can simply be selected from the list and additional parameters (e.g. security credentials, frequency band) can then be configured instead of having to manually configure all parameters.

Ensure that the selected SSID is not utilized by any other wireless LANs as that could lead to failures when powering on or during roaming; especially if a different security type is utilized.



WLANs > Edit 'voice'

Profile Name voice

Type WLAN

SSID voice

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X + CCKM)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11a only

Interface/Interface Group(G) voice

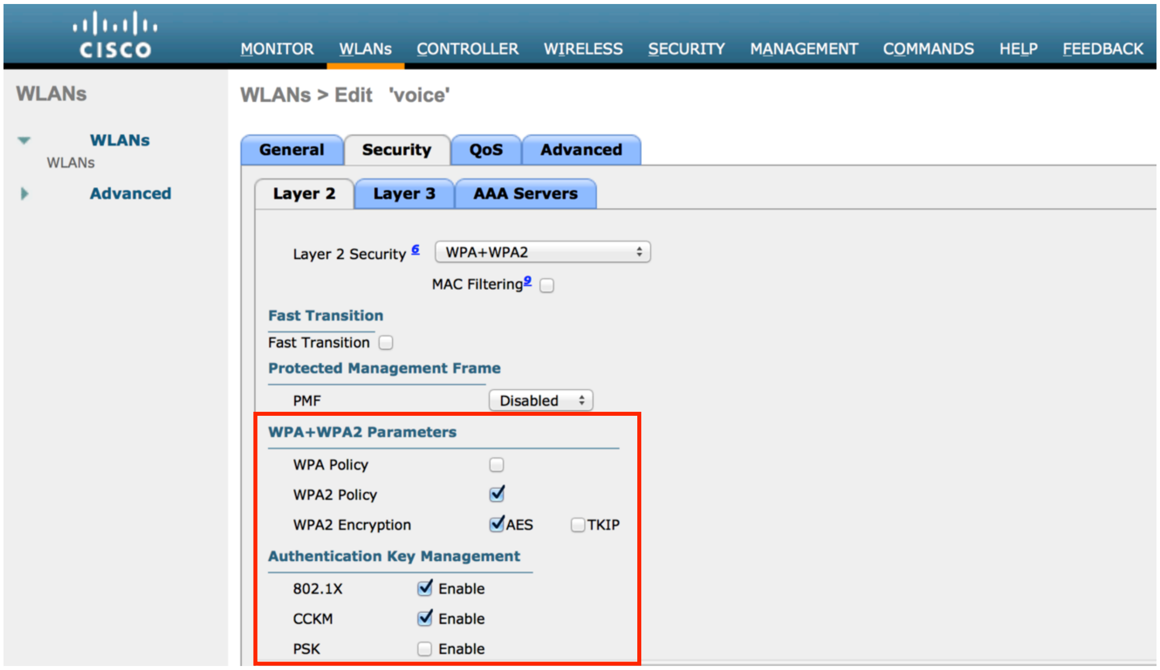
Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☑ Enabled

NAS-ID WLC5508-1

In order to utilize CCKM, enable WPA2 policy with AES encryption and 802.1x + CCKM for authenticated key management type in order to enable fast secure roaming.

Cisco Cius also supports WPA(TKIP) with 802.1x + CCKM key-management, but WPA2(AES) with 802.1x + CCKM key-management is the recommended configuration.



WLANs > Edit 'voice'

Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] □

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy	□	
WPA2 Policy	☑	
WPA2 Encryption	☑AES	□TKIP

Authentication Key Management

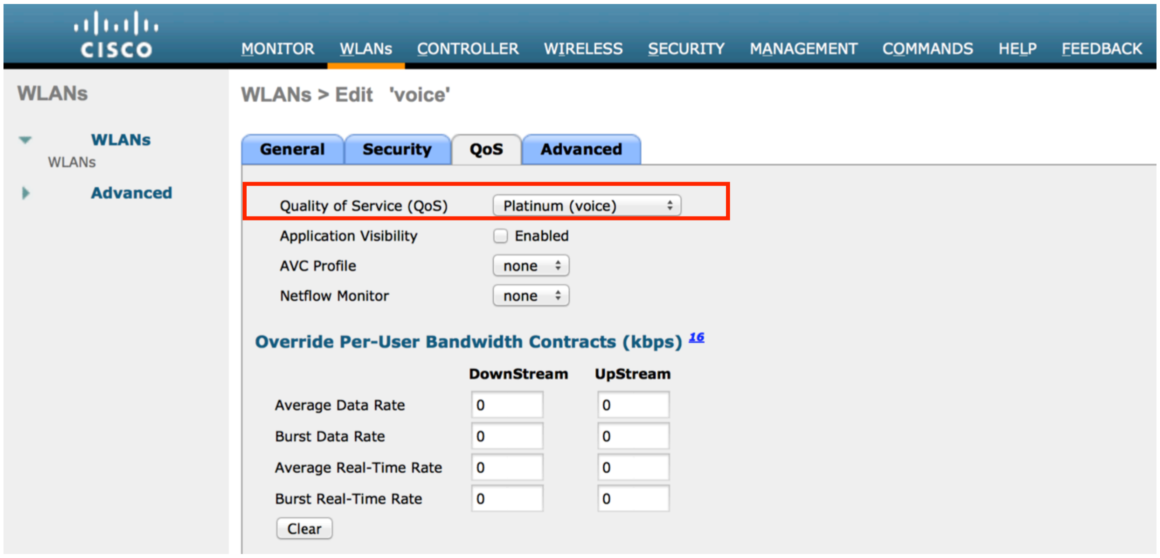
802.1X	☑ Enable
CCKM	☑ Enable
PSK	□ Enable

The WMM policy should be set to **Required** only if Cisco Cius or other WMM enabled voice and/or video capable endpoints will be using this SSID.

If there are non-WMM clients existing in the WLAN, it is recommended to put those clients on another SSID / WLAN.

If non-other WMM clients must utilize the same SSID as Cisco Cius, then ensure the WMM policy is set to **Allowed.**

Enable **7920 AP CAC** to advertise Qos Basic Service Set (QBSS) to the client.



WLANs > Edit 'voice'

Quality of Service (QoS) Platinum (voice)

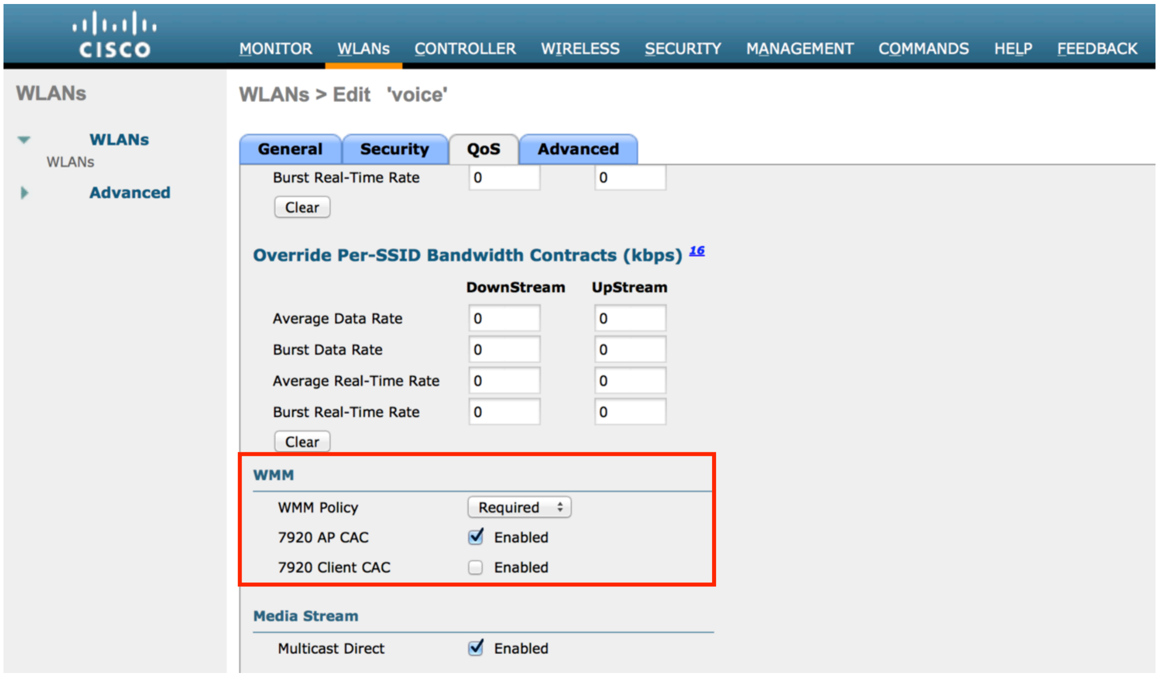
Application Visibility □ Enabled

AVC Profile none

Netflow Monitor none

Override Per-User Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0



WLANs > Edit 'voice'

Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WMM

WMM Policy	Required
7920 AP CAC	☑ Enabled
7920 Client CAC	□ Enabled

Media Stream

Multicast Direct	☑ Enabled

Configure **Enable Session Timeout** as necessary per your requirements. It is recommended to either disable the session timeout or extend the timeout (e.g. 24 hours / 86400 seconds) to avoid possible interruptions during audio or video calls. If disabled it will avoid any potential interruptions altogether, but enabling session timeout can help to re-validate client credentials periodically to ensure that the client is using valid credentials.

Enable Aironet Extensions (**Aironet IE).**

Peer to Peer (P2P) Blocking Action should be disabled.

Configure **Client Exclusion** as necessary.

Off Channel Scanning Defer can be tuned to defer scanning for certain queues as well as the scan defer time.

If using best effort applications frequently (e.g. web browsing, VPN, etc.) or if DSCP values for priority applications (e.g. voice, video, call control) are not preserved to the access point, then is recommended to enable the lower priority queues (0-3) along with the higher priority queues (4-6) to defer off channel scanning as well as potentially increasing the scan defer time.

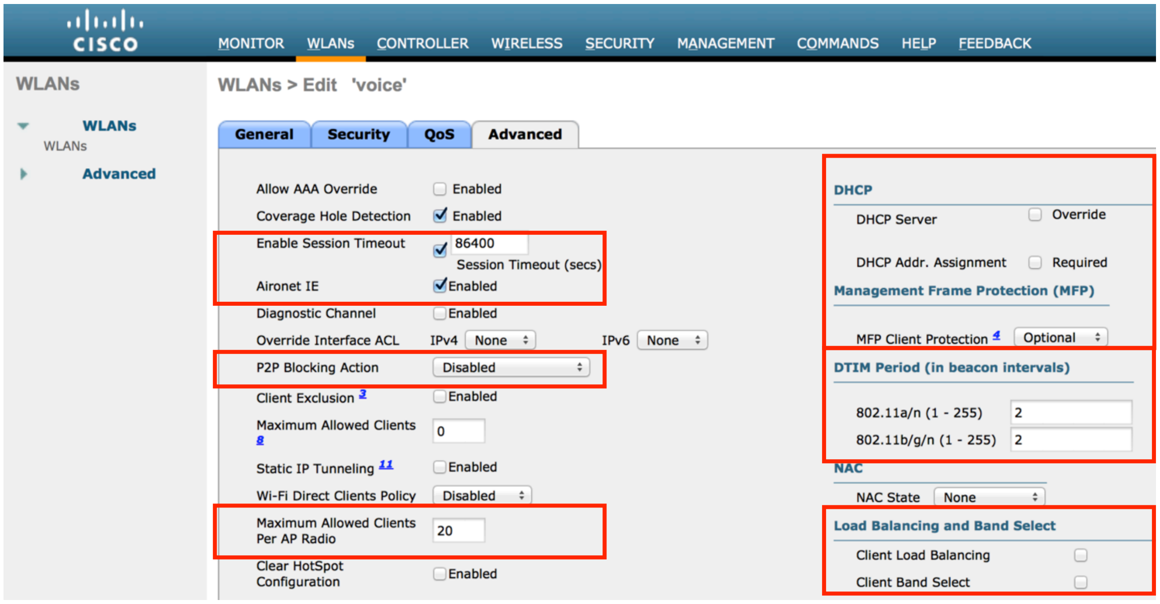
The **Maxium Allowed Clients Per AP Radio** can be configured as necessary.

DHCP Address Assignment Required should be disabled.

Management Frame Protection should be set to **Optional** or **Disabled.**

For optimal battery performance and quality, use a **DTIM Period** of **2** with a beacon period of **100 ms**.

Ensure **Client Load Balancing** and **Client Band Select** are disabled for the voice SSID.


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Advanced

WLANs > Edit 'voice'

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 86400 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion [3] □ Enabled
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 20
Clear HotSpot Configuration □ Enabled

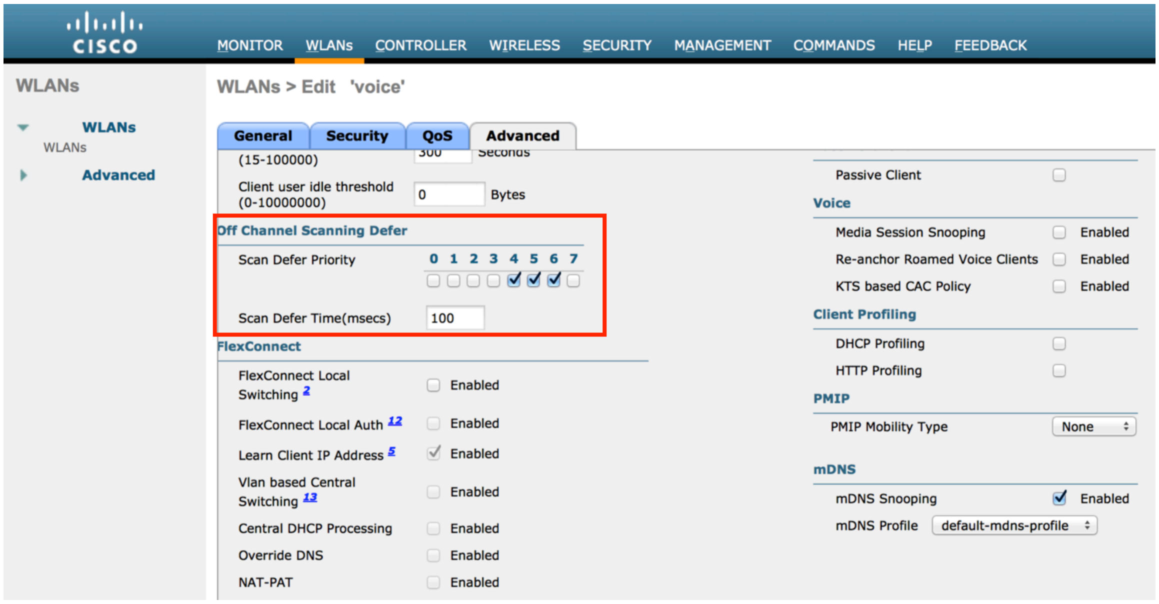
DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 2
802.11b/g/n (1 - 255) 2

NAC
NAC State None

Load Balancing and Band Select
Client Load Balancing □
Client Band Select □


cisco
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Advanced

WLANs > Edit 'voice'

(15-100000) 300 Seconds
Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer
Scan Defer Priority 0 1 2 3 4 5 6 7
□ □ □ □ ☑ ☑ ☑ □
Scan Defer Time(msecs) 100

FlexConnect
FlexConnect Local Switching [2] □ Enabled
FlexConnect Local Auth [12] □ Enabled
Learn Client IP Address [5] ☑ Enabled
Vlan based Central Switching [13] □ Enabled
Central DHCP Processing □ Enabled
Override DNS □ Enabled
NAT-PAT □ Enabled

Passive Client □

Voice
Media Session Snooping □ Enabled
Re-anchor Roamed Voice Clients □ Enabled
KTS based CAC Policy □ Enabled

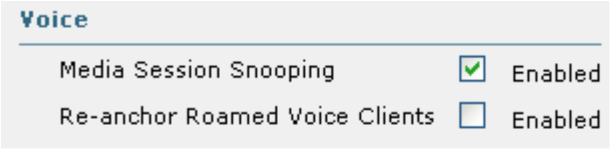
Client Profiling
DHCP Profiling □
HTTP Profiling □

PMIP
PMIP Mobility Type None

mDNS
mDNS Snooping ☑ Enabled
mDNS Profile default-mdns-profile

Media Session Snooping can be enabled to utilize SIP CAC.

It is recommended to set **Re-anchor Roamed Voice Clients** to disabled as this can cause brief interruptions with wireless LAN connectivity when a call is terminated after performing an inter-controller roaming.



Voice
Media Session Snooping ☑ Enabled
Re-anchor Roamed Voice Clients □ Enabled

For the Cisco Autonomous Access Point, ensure that the SSID is configured for open + eap as and network-eap when using 802.1x authentication.

```
dot11 ssid voice
   vlan 21
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa cckm
   admit-traffic
```

If the Cisco Autonomous Access Point is registered to a WDS (Wireless Domain Services) server, ensure both types of authentication are enabled in the WDS configuration.

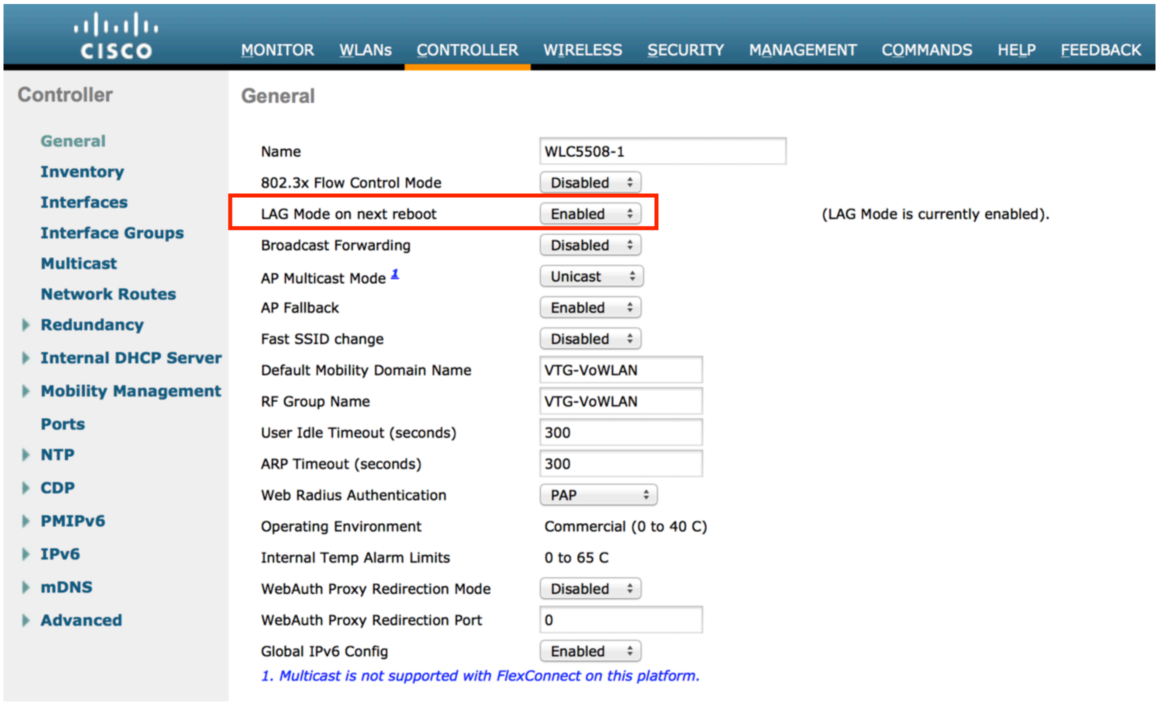
```
wlccp authentication-server infrastructure method_Infrastructure
wlccp authentication-server client mac method_Clients
wlccp authentication-server client eap method_Clients
wlccp authentication-server client leap method_Clients
wlccp wds priority 255 interface BVI1
```

Controller Settings

Ensure the Cisco Unified Wireless LAN Controller hostname is configured correctly.

Enable Link Aggregation (LAG) if utilizing multiple ports on the Cisco Unified Wireless LAN Controller.

Configure the desired AP multicast mode.

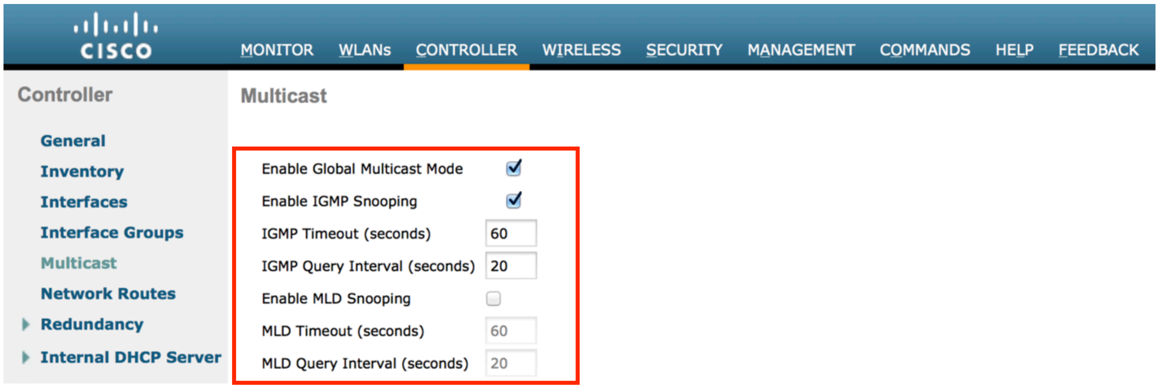


General

Name	WLC5508-1
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled (LAG Mode is currently enabled).
Broadcast Forwarding	Disabled
AP Multicast Mode [1]	Unicast
AP Fallback	Enabled
Fast SSID change	Disabled
Default Mobility Domain Name	VTG-VoWLAN
RF Group Name	VTG-VoWLAN
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled
WebAuth Proxy Redirection Port	0
Global IPv6 Config	Enabled

1. Multicast is not supported with FlexConnect on this platform.

If utilizing multicast, then **Enable Global Multicast Mode** and **Enable IGMP Snooping** should be enabled.

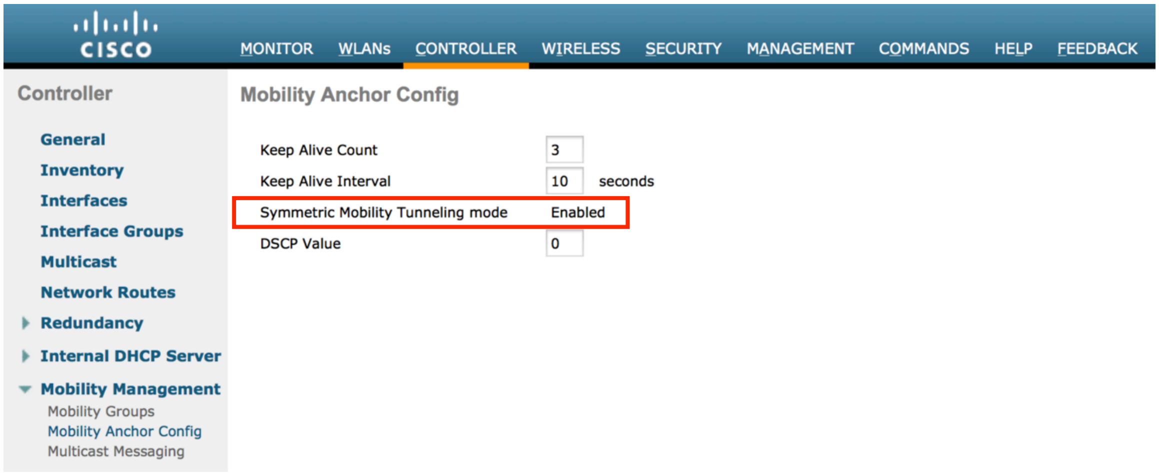


Multicast

Enable Global Multicast Mode	☑
Enable IGMP Snooping	☑
IGMP Timeout (seconds)	60
IGMP Query Interval (seconds)	20
Enable MLD Snooping	□
MLD Timeout (seconds)	60
MLD Query Interval (seconds)	20

If utilizing layer 3 mobility, then **Symmetric Mobility Tunneling** should be **Enabled**.

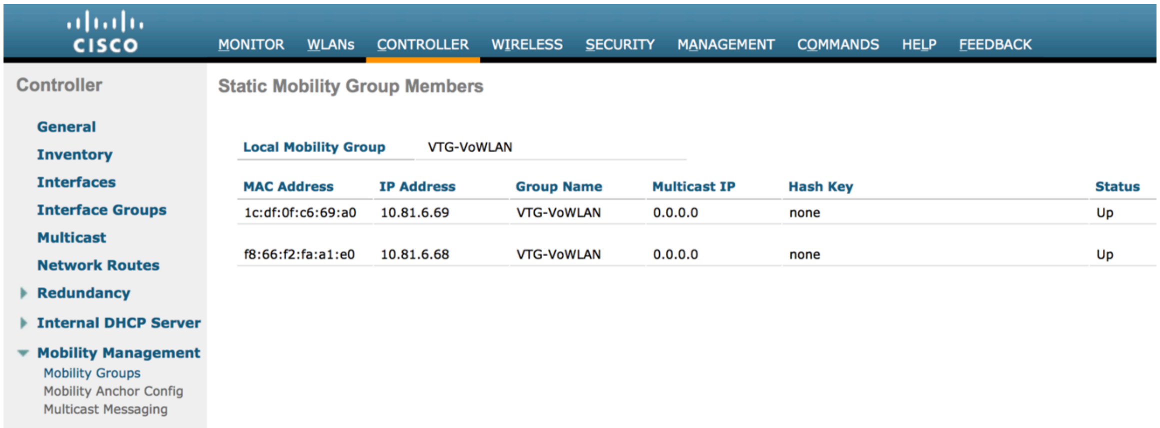
In the recent versions, Symmetric Mobility Tunneling is enabled by default and non-configurable.



Mobility Anchor Config

Keep Alive Count	3
Keep Alive Interval	10 seconds
Symmetric Mobility Tunneling mode	Enabled
DSCP Value	0

When multiple Cisco Unified Wireless LAN Controllers are to be in the same mobility group, then the IP address and MAC address of each Cisco Unified Wireless LAN Controller should be added to the Static Mobility Group Members configuration.



Static Mobility Group Members

Local Mobility Group VTG-VoWLAN

MAC Address	IP Address	Group Name	Multicast IP	Hash Key	Status
1c:df:0f:c6:69:a0	10.81.6.69	VTG-VoWLAN	0.0.0.0	none	Up
f8:66:f2:fa:a1:e0	10.81.6.68	VTG-VoWLAN	0.0.0.0	none	Up

802.11 Network Settings

If using 5 GHz, ensure the 802.11a network status is **Enabled**.

Set the **Beacon Period** to **100 ms**.

Ensure **DTPC Support** is enabled.

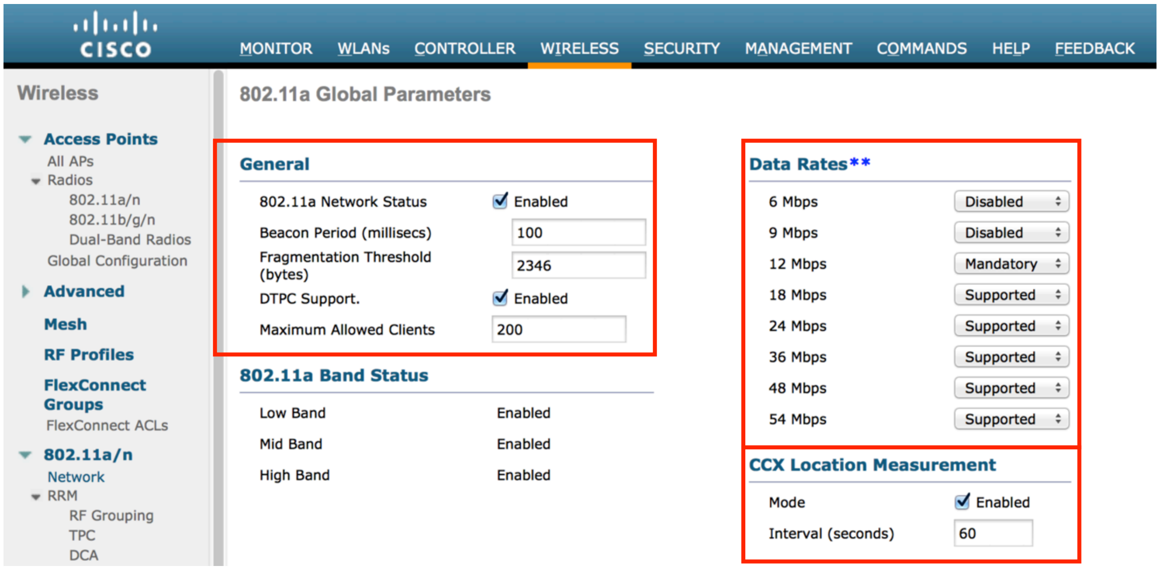
If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

With the current releases, **Maximum Allowed Clients** can be configured.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18-24 or 18-54 Mbps as supported (optional) rates; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

36-54 Mbps can optionally be disabled, if there are not any applications that can benefit from those rates (e.g. video).

Enable **CCX Location Measurement**.



802.11a Global Parameters

General

802.11a Network Status	☑ Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200

802.11a Band Status

Low Band	Enabled
Mid Band	Enabled
High Band	Enabled

Data Rates**

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

If using 2.4 GHz, ensure the 802.11b/g/n network status and 802.11g/n is enabled.

Set the **Beacon Period** to **100 ms**.

Short Preamble should be **Enabled** in the 2.4 GHz radio configuration setting on the access point when no legacy clients that require a long preamble are present in the wireless LAN. By using the short preamble instead of long preamble, the wireless network performance is improved.

Ensure **DTPC Support** is enabled.

If using Cisco 802.11n Access Points, ensure **ClientLink** is enabled.

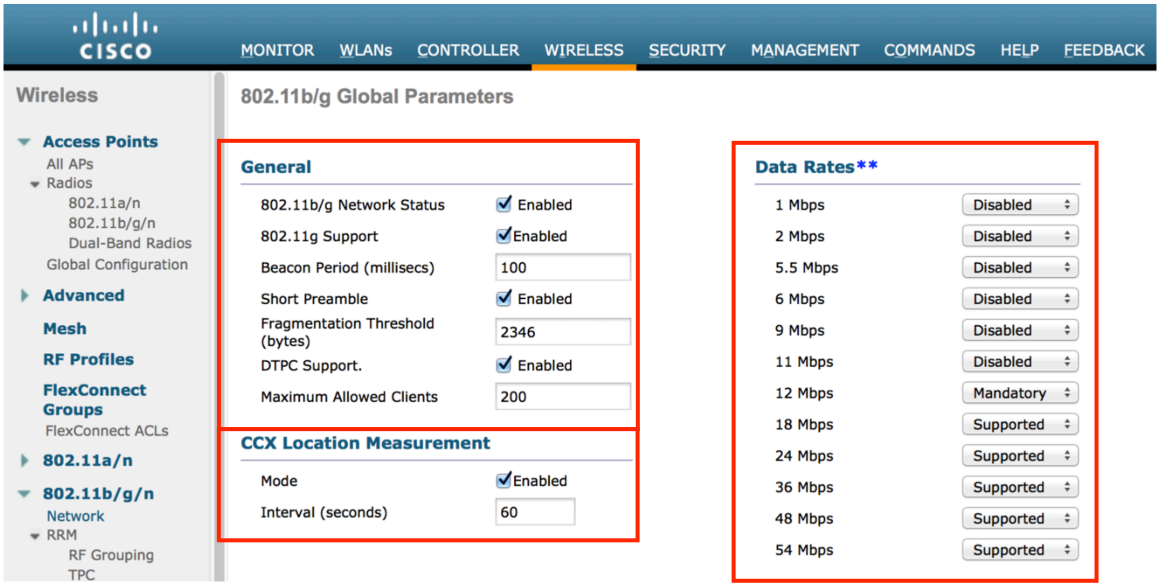
With the current releases, **Maximum Allowed Clients** can be configured.

Recommended to set 12 Mbps as the mandatory (basic) rate and 18-24 or 18-54 Mbps as supported (optional) rates assuming that there will not be any 802.11b only clients that will connect to the wireless LAN; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

If 802.11b clients exist, then 11 Mbps should be set as the mandatory (basic) rate and 12-24 or 54 Mbps as supported (optional).

36-54 Mbps can optionally be disabled, if there are not any applications that can benefit from those rates (e.g. video).

Enable **CCX Location Measurement**.



802.11b/g Global Parameters

General

802.11b/g Network Status	☑ Enabled
802.11g Support	☑ Enabled
Beacon Period (millisecs)	100
Short Preamble	☑ Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200

CCX Location Measurement

Mode	☑ Enabled
Interval (seconds)	60

Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

Beamforming (ClientLink)

Enable **ClientLink** if using Cisco 802.11n Access Points.

Beamforming is not supported with data rates 1, 2, 5.5, and 11 Mbps.

For releases prior to 7.2.103.0, **ClientLink** can be enabled globally via the 802.11 Global Parameters section or on individual access points via the access point's 802.11 radio configuration page.

As of release 7.2.103.0, **ClientLink** is no longer configurable via the Cisco Unified Wireless LAN Controller's web interface and is only configurable via command line.

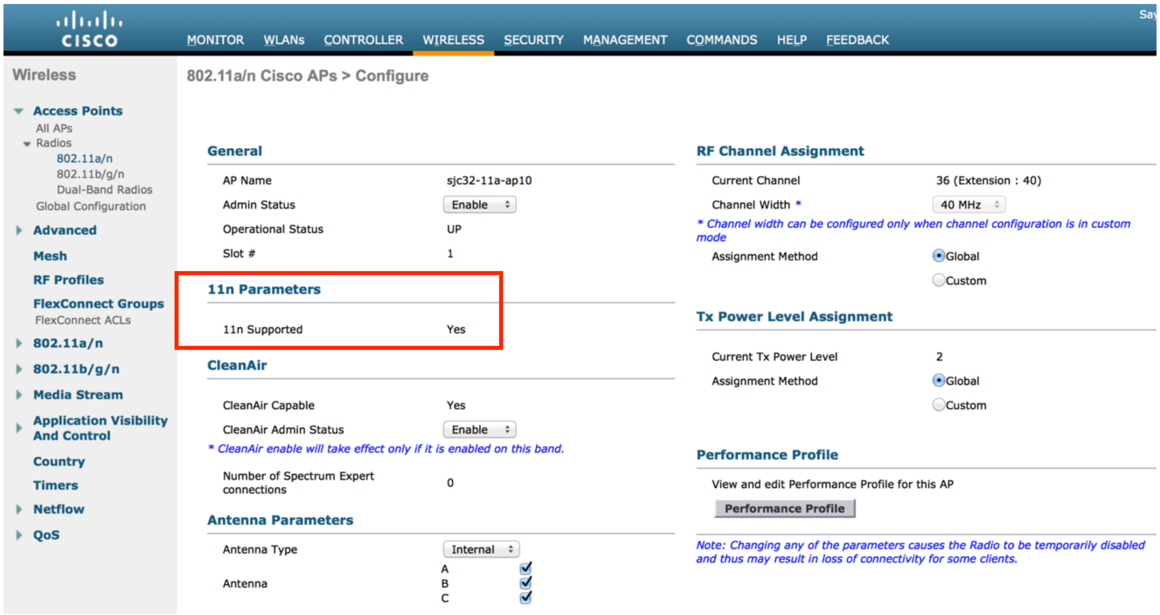
With releases 7.2.103.0 and later use the following commands to enable the beamforming feature globally for all access points or for individual access point radios.

```
(Cisco Controller) >config 802.11a beamforming global enable
(Cisco Controller) >config 802.11a beamforming ap <ap_name> enable
(Cisco Controller) >config 802.11b beamforming global enable
(Cisco Controller) >config 802.11b beamforming ap <ap_name> enable
```

The current status of the beamforming feature can be displayed by using the following command.

```
(Cisco Controller) >show 802.11a
(Cisco Controller) >show 802.11b

Legacy Tx Beamforming setting................... Enabled
```



802.11a/n Cisco APs > Configure

General

AP Name	sjc32-11a-ap10
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	36 (Extension : 40)
Channel Width *	40 MHz

* Channel width can be configured only when channel configuration is in custom mode

Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	2
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

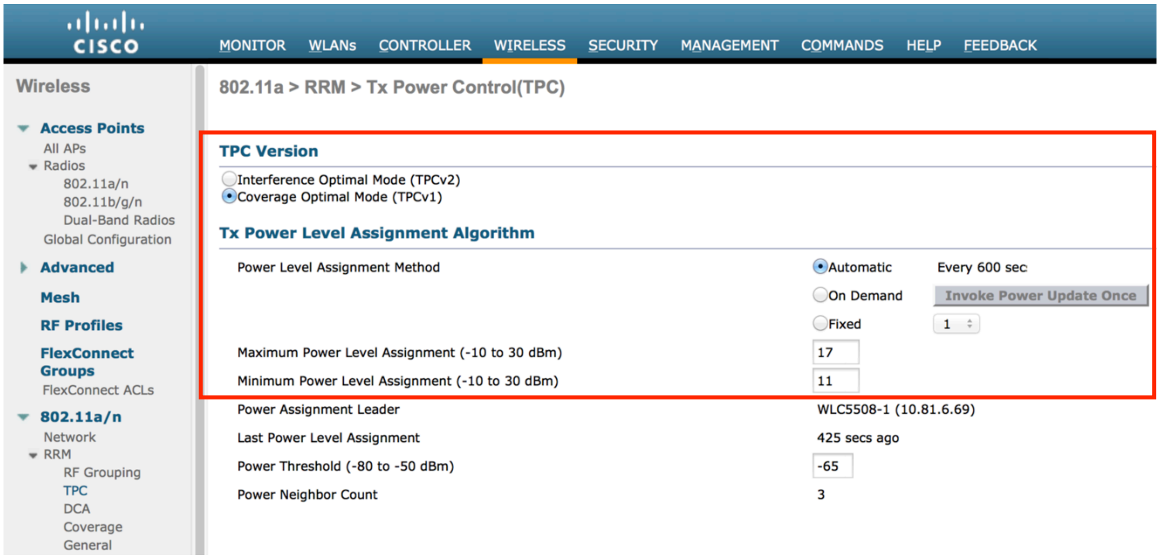
Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Auto RF (RRM)

When using the Cisco Unified Wireless LAN Controller it is recommended to enable Auto RF to manage the channel and transmit power settings.

Configure the access point transmit power level assignment method for either 5 or 2.4 GHz depending on which band is to be utilized.

If using automatic power level assignment, a maximum and minimum power level can be specified.



802.11a > RRM > Tx Power Control(TPC)

TPC Version

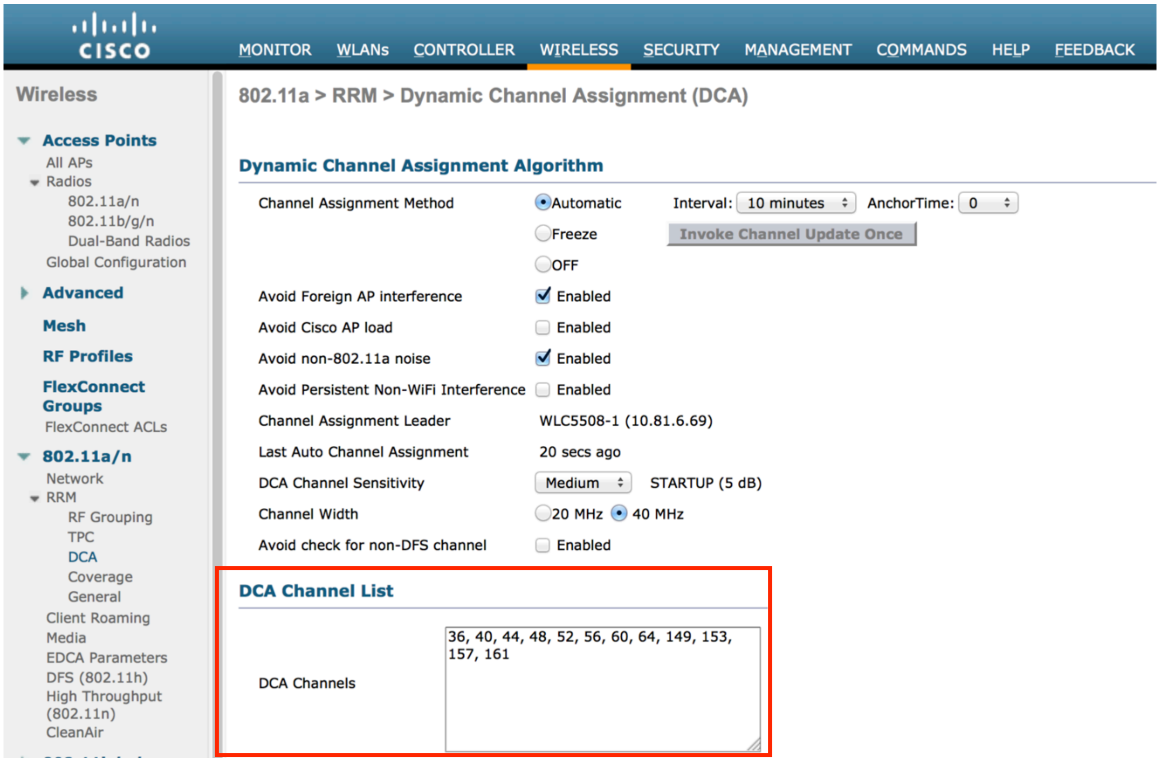
○ Interference Optimal Mode (TPCv2)
● Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method	● Automatic	Every 600 sec
	○ On Demand	Invoke Power Update Once
	○ Fixed	1
Maximum Power Level Assignment (-10 to 30 dBm)	17	
Minimum Power Level Assignment (-10 to 30 dBm)	11	
Power Assignment Leader	WLC5508-1 (10.81.6.69)	
Last Power Level Assignment	425 secs ago	
Power Threshold (-80 to -50 dBm)	-65	
Power Neighbor Count	3	

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

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



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic ○ Freeze ○ OFF Interval: 10 minutes AnchorTime: 0

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load □ Enabled

Avoid non-802.11a noise ☑ Enabled

Avoid Persistent Non-WiFi Interference □ Enabled

Channel Assignment Leader WLC5508-1 (10.81.6.69)

Last Auto Channel Assignment 20 secs ago

DCA Channel Sensitivity Medium STARTUP (5 dB)

Channel Width ○ 20 MHz ● 40 MHz

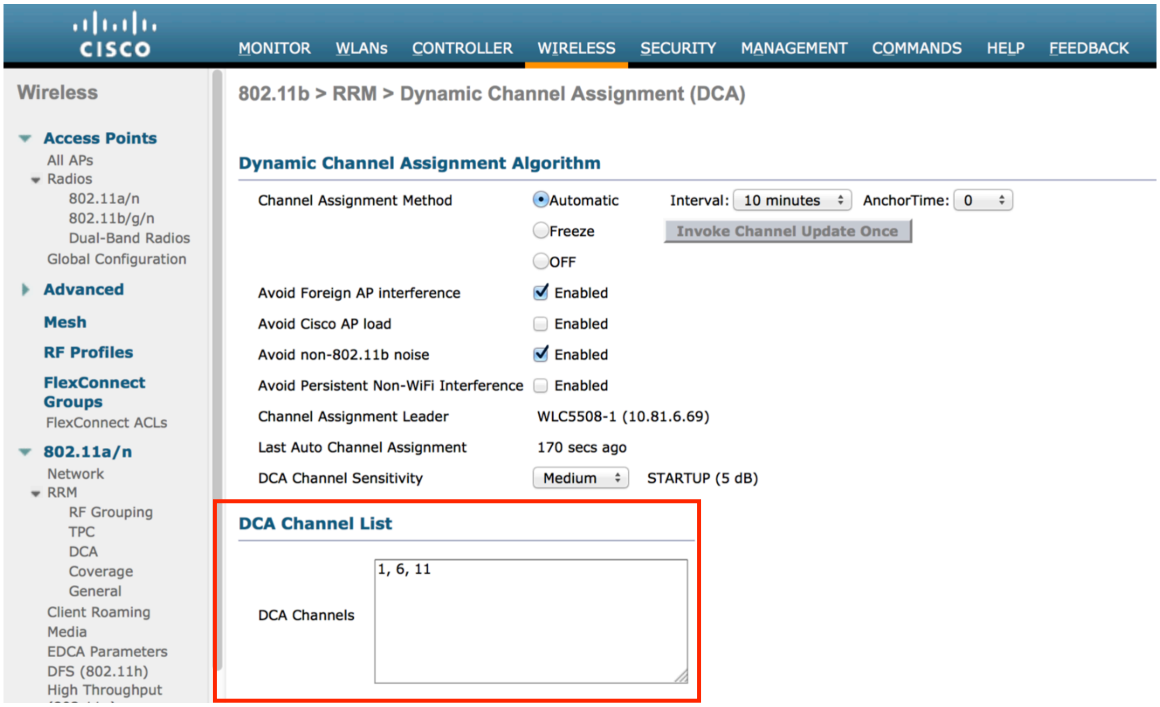
Avoid check for non-DFS channel □ Enabled

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

If using 2.4 GHz, only channels 1, 6, and 11 should be enabled in the DCA list.

It is recommended to configure the 2.4 GHz channel for 20 MHz even if using Cisco 802.11n Access Points capable of 40 MHz due to the limited number of channels available in 2.4 GHz.



802.11b > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic ○ Freeze ○ OFF Interval: 10 minutes AnchorTime: 0

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load □ Enabled

Avoid non-802.11b noise ☑ Enabled

Avoid Persistent Non-WiFi Interference □ Enabled

Channel Assignment Leader WLC5508-1 (10.81.6.69)

Last Auto Channel Assignment 170 secs ago

DCA Channel Sensitivity Medium STARTUP (5 dB)

DCA Channel List

DCA Channels 1, 6, 11

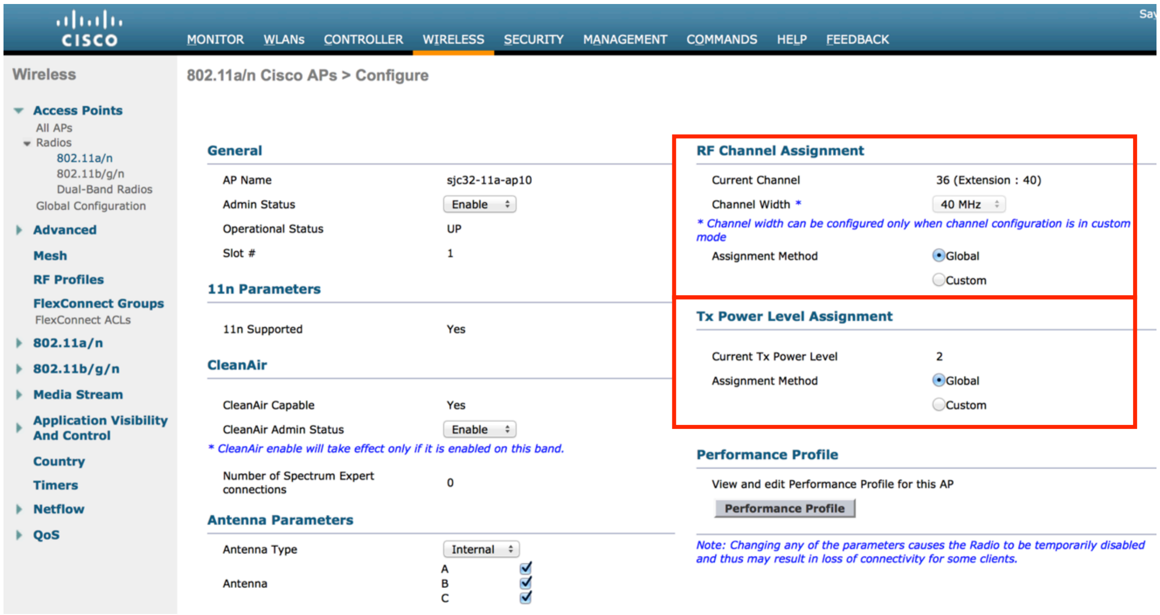
Individual access points can be configured to override the global setting to use dynamic channel and transmit power assignment for either 5 or 2.4 GHz depending on which band is to be utilized.

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

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

The channel width can be configured for 20 MHz or 40 MHz if using Cisco 802.11n Access Points.

It is recommended to use 40 MHz channels only if using 5 GHz.



802.11a/n Cisco APs > Configure

General

AP Name	sjc32-11a-ap10
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

* CleanAir enable will take effect only if it is enabled on this band.

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	36 (Extension : 40)
Channel Width *	40 MHz

* Channel width can be configured only when channel configuration is in custom mode

Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	2
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Client Roaming

Cisco Cius does not utilize the RF parameters in the Client Roaming section of the Cisco Unified Wireless LAN Controller as scanning and roaming is managed independently by the phone itself.

Call Admission Control

Cisco Cius currently does not support TSPEC (Call Admission Control).

Call Admission Control (TSPEC) for voice should only be enabled if other TSPEC capable clients are using the same band frequency; TSPEC for video should not be enabled.

If **Admission Control Mandatory (ACM)** is enabled for **Voice**, Cisco Cius will be required to downgrade the priority of the audio packets sent upstream from UP6 (voice) to a lower priority (UP5 video) for an audio only call.

If Call Admission Control for voice is to be enabled, then configure maximum bandwidth and reserved roaming bandwidth percentages for either 5 or 2.4 GHz depending on which band is to be utilized.

The maximum bandwidth default setting for voice is **75%** where **6%** of that bandwidth is reserved for roaming clients.

Roaming clients are not limited to using the reserved roaming bandwidth, but roaming bandwidth is to reserve some bandwidth for roaming clients in case all other bandwidth is utilized.

If CAC is to be enabled, will want to ensure **Load-based CAC** is enabled, which is available for the Cisco Unified Wireless LAN Controller, but not currently available on the Cisco Autonomous Access Point platform.

Load-based CAC will account for non-TSPEC clients as well as all other energy on the channel.

Since TSPEC is not supported currently, **SIP CAC** can be utilized, which will require media session snooping to be enabled on the WLAN / SSID.

Traffic Stream Metrics (TSM) is not supported as this feature requires TSPEC support, but can be enabled if other capable clients are utilizing the same band frequency.

SIP CAC is to help ensure that downstream voice frames are prioritized correctly.

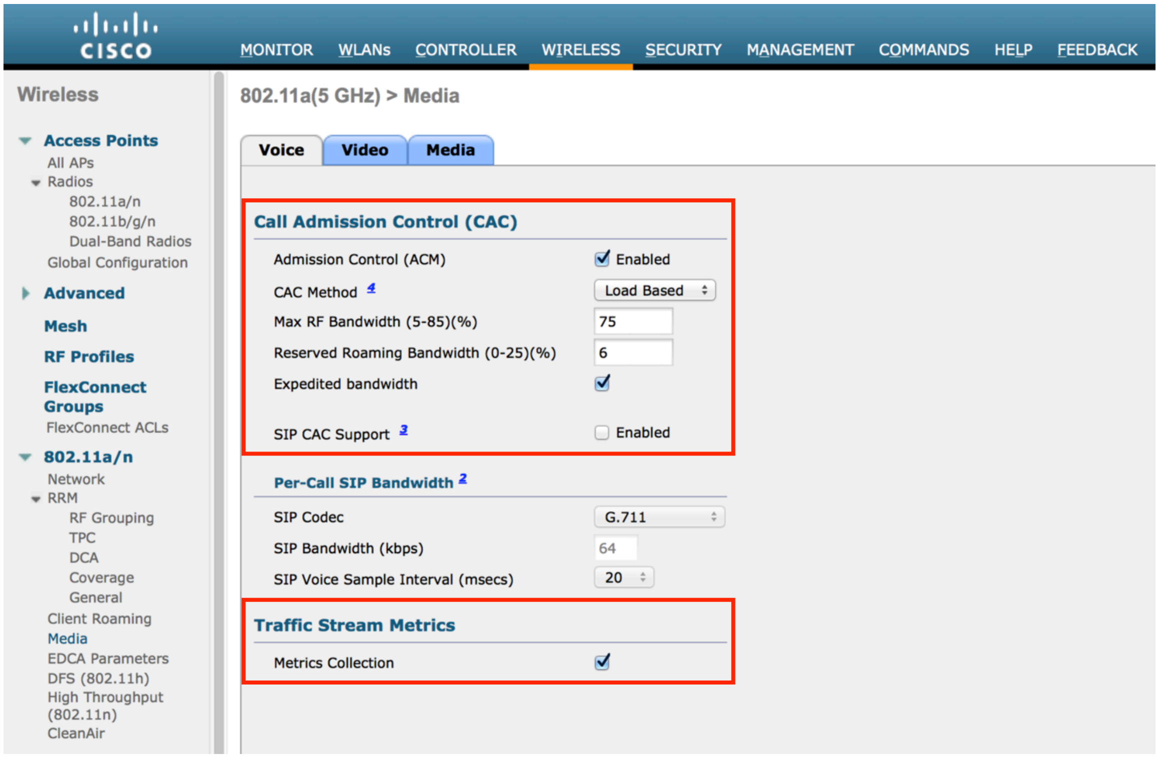
Load based CAC logic is utilized with SIP CAC, so all 802.11 traffic and energy on the channel is accounted for to determine available bandwidth.

The access point has different methods for call admission control when using SIP CAC depending on whether the client uses TCP or UDP for SIP communications.

If the client uses TCP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN / SSID and will not forward the SIP frames upstream or downstream if there is not bandwidth available for the new voice stream. This could potentially result in loss of registration to the Cisco Unified Communications Manager.

If the client uses UDP for SIP, then the access point will snoop the SIP packets when media session snooping is enabled on the WLAN / SSID and will sent a 486 busy message to the client, which in turn can be interpreted as a **Network Busy** message and the client could either roam to another access point or simply terminate the call setup for that session.

Cisco Cius uses TCP for SIP communications, therefore if the channel is busy where another call can not be allowed, then Cisco Cius could potentially lose registration to the Cisco Unified Communications Manager.



802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM) ☑ Enabled

CAC Method 4 Load Based

Max RF Bandwidth (5-85)(%) 75

Reserved Roaming Bandwidth (0-25)(%) 6

Expedited bandwidth ☑

SIP CAC Support 3 ☐ Enabled

Per-Call SIP Bandwidth 2

SIP Codec G.711

SIP Bandwidth (kbps) 64

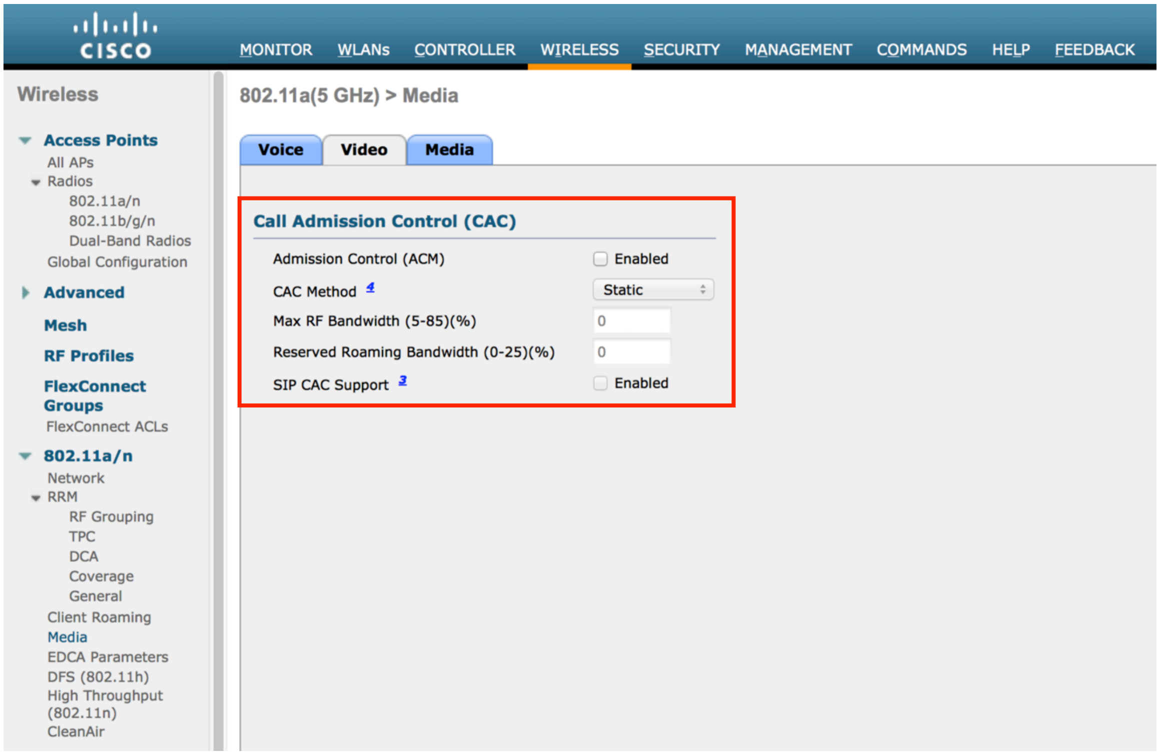
SIP Voice Sample Interval (msecs) 20

Traffic Stream Metrics

Metrics Collection ☑

Admission Control Mandatory for **Video** should be disabled.

If enabled, priority of video frames will be downgraded to best effort.



802.11a(5 GHz) > Media

Call Admission Control (CAC)

Admission Control (ACM)	□ Enabled
CAC Method [4]	Static
Max RF Bandwidth (5-85)(%)	0
Reserved Roaming Bandwidth (0-25)(%)	0
SIP CAC Support [3]	□ Enabled

If Call Admission Control for voice is enabled, then the following configuration should be enabled, which can be displayed in the **show run-config**.

```
Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM)............ Enabled
Voice max RF bandwidth....................... 75
Voice reserved roaming bandwidth............. 6
Voice load-based CAC mode.................... Enabled
Voice tspec inactivity timeout................ Disabled
Video AC - Admission control (ACM)............ Disabled
Voice Stream-Size........................... 84000
Voice Max-Streams............................ 2
Video max RF bandwidth....................... 25
Video reserved roaming bandwidth............. 6
```

The voice stream-size and voice max-streams values can be adjusted as necessary by using the following command.

```
(Cisco Controller) >config 802.11a cac voice stream-size 84000 max-streams 2
```

Ensure QoS is setup correctly under the WLAN / SSID configuration, which can be displayed by using the following command.

```
(Cisco Controller) >show wlan <WLAN id>
```

```
Quality of Service............................. Platinum (voice)
WMM............................................ Allowed
```

Dot11-Phone Mode (7920).......................... ap-cac-limit
Wired Protocol.................................. 802.1P (Tag=6)

When enabling Call Admission Control on the Cisco Autonomous Access Point, the admission must be unblocked on the SSID as well.

It is required to enable Call Admission Control on the SSID configuration, regardless of Admission Control being enabled for voice or video.

Load-based CAC and support for multiple streams are 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 1 stream and the stream size is not customizable, therefore SRTP and barge will not work if CAC is enabled.

```
dot11 ssid voice
  vlan 21
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa cckm
  admit-traffic
```

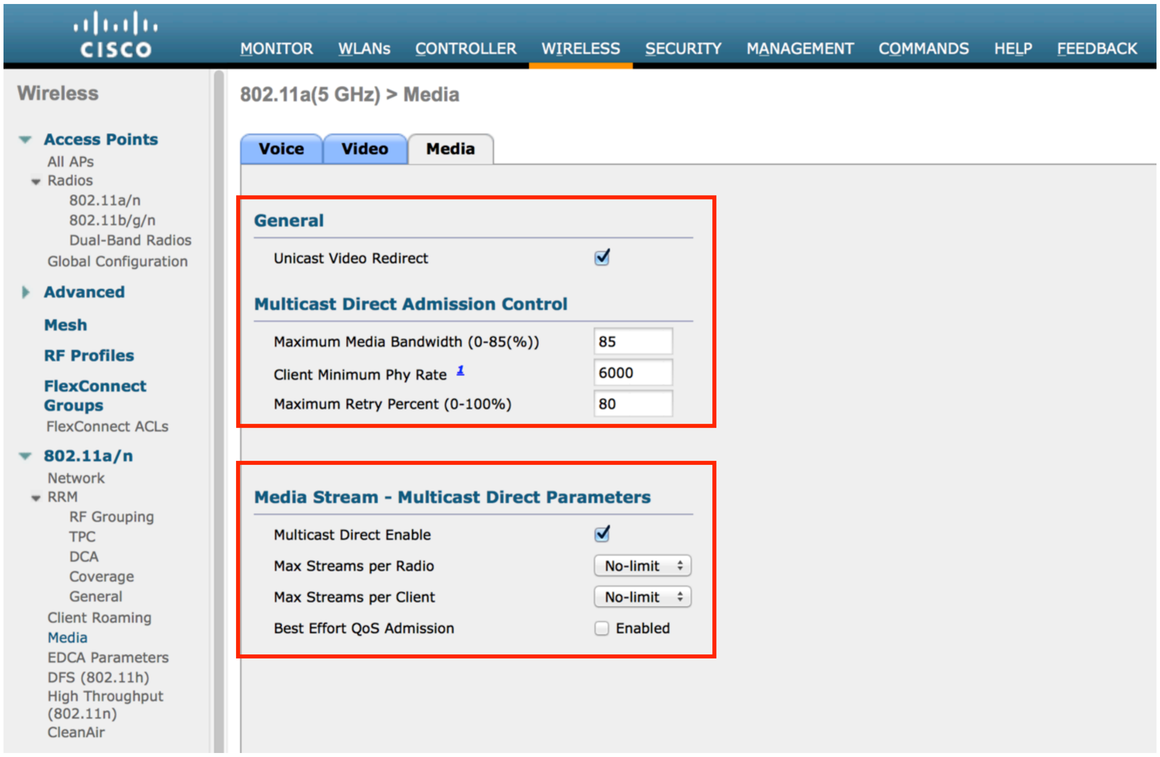
It is recommended to use the defaults, where 5.5, 6.0, 11.0, 12.0 and 24.0 Mbps are enabled as nominal rates for 802.11b/g and 6.0, 12.0 and 24.0 Mbps enabled for 802.11a.

If enabling the STREAM feature either directly or via selecting **Optimized Voice** for the radio access category in the QoS configuration section, 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.

For more information about Call Admission Control and QoS, refer to the **Configuring QoS** chapter in the Cisco IOS Software Configuration Guide for Cisco Aironet Access Points at this URL:

http://www.cisco.com/en/US/partner/docs/wireless/access_point/12.4.25d.JA/Configuration/guide/scg12.4.25d.JA-chap15-qos.html

In the Media settings, **Unicast Video Redirect** and **Multicast Direct Enable** should be enabled.



802.11a(5 GHz) > Media

General

Unicast Video Redirect ☑

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))	85
Client Minimum Phy Rate	6000
Maximum Retry Percent (0-100%)	80

Media Stream - Multicast Direct Parameters

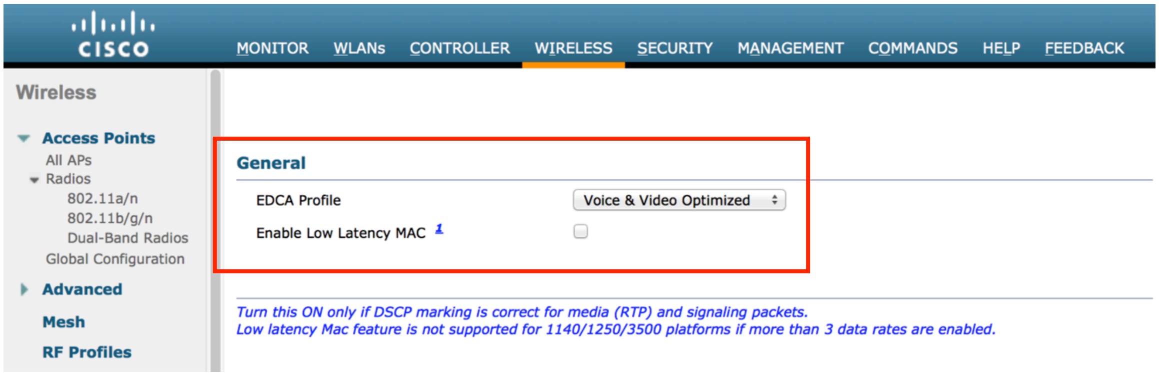
Multicast Direct Enable	☑
Max Streams per Radio	No-limit
Max Streams per Client	No-limit
Best Effort QoS Admission	□ Enabled

EDCA Parameters

Set the EDCA profile for **Voice and Video Optimized** and disable **Low Latency MAC** for either 5 or 2.4 GHz depending on which band is to be utilized.

Low Latency MAC (LLM) reduces the number of retransmissions to 2-3 per packet depending on the access point platform, so it can cause issues if multiple data rates are enabled.

LLM is not supported on the Cisco 802.11n Access Points.



General

EDCA Profile	Voice & Video Optimized
Enable Low Latency MAC	□

Turn this ON only if DSCP marking is correct for media (RTP) and signaling packets.
Low latency Mac feature is not supported for 1140/1250/3500 platforms if more than 3 data rates are enabled.

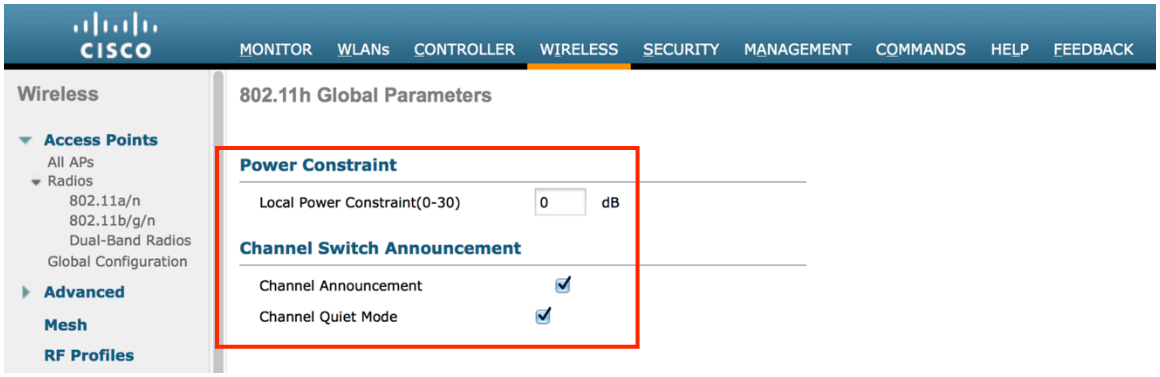
DFS (802.11h)

In the DFS (802.11h) configuration, channel announcement and quiet mode should be enabled.

Power Constraint should be left un-configured or set to 0 dBm as DTPC will be used by Cisco Cius to control the transmission power.

In later versions of the Cisco Unified Wireless LAN Controller it does not allow both TPC (Power Constraint) and DTPC (Dynamic Transmit Power Control) to be enabled simultaneously.

Channel Announcement and **Channel Quiet Mode** should be enabled.



802.11h Global Parameters

Power Constraint

Local Power Constraint(0-30) 0 dB

Channel Switch Announcement

Channel Announcement ☑

Channel Quiet Mode ☑

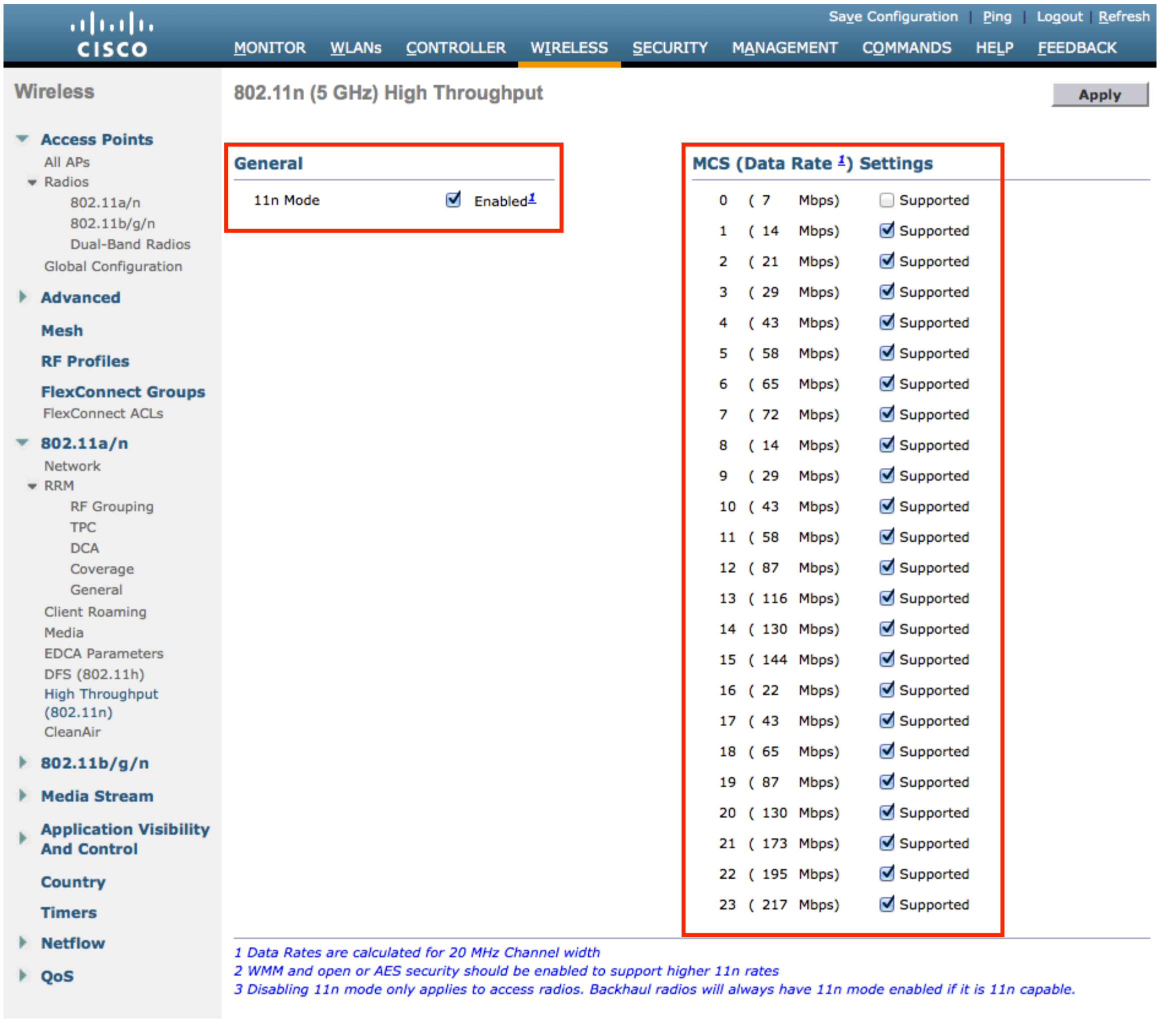
High Throughput (802.11n)

The 802.11n data rates can be configured per radio (2.4 GHz and 5 GHz).

Ensure that **WMM** is enabled and **WPA2(AES)** is configured in order to utilize 802.11n data rates.

Cisco Cius supports MCS 0 - MCS 7 data rates only, but MCS 8 - MCS 15 can optionally be enabled if there are other 802.11n clients utilizing the same band frequency that include MIMO antenna technology, which can take advantage of the those higher data rates.

It is recommended to disable MCS 0.



802.11n (5 GHz) High Throughput

General

11n Mode ☑ Enabled[1]

MCS (Data Rate [1]) Settings

0	(7 Mbps)	□ Supported
1	(14 Mbps)	☑ Supported
2	(21 Mbps)	☑ Supported
3	(29 Mbps)	☑ Supported
4	(43 Mbps)	☑ Supported
5	(58 Mbps)	☑ Supported
6	(65 Mbps)	☑ Supported
7	(72 Mbps)	☑ Supported
8	(14 Mbps)	☑ Supported
9	(29 Mbps)	☑ Supported
10	(43 Mbps)	☑ Supported
11	(58 Mbps)	☑ Supported
12	(87 Mbps)	☑ Supported
13	(116 Mbps)	☑ Supported
14	(130 Mbps)	☑ Supported
15	(144 Mbps)	☑ Supported
16	(22 Mbps)	☑ Supported
17	(43 Mbps)	☑ Supported
18	(65 Mbps)	☑ Supported
19	(87 Mbps)	☑ Supported
20	(130 Mbps)	☑ Supported
21	(173 Mbps)	☑ Supported
22	(195 Mbps)	☑ Supported
23	(217 Mbps)	☑ Supported

1 Data Rates are calculated for 20 MHz Channel width
2 WMM and open or AES security should be enabled to support higher 11n rates
3 Disabling 11n mode only applies to access radios. Backhaul radios will always have 11n mode enabled if it is 11n capable.

Frame Aggregation

Frame aggregation is a process of packaging multiple MAC Protocol Data Units (MPDUs) or MAC Service Data Units (MSDUs) together to reduce the overheads where in turn throughput and capacity can be optimized.
Aggregation of MAC Protocol Data Unit (A-MPDU) requires the use of block acknowledgements.

It is recommended to adjust the A-MPDU and A-MSDU settings to the following to optimize the Cisco Cius experience.

A-MPDU
User Priority 0, 3, 4, 5 = Enabled
User Priority 1, 2, 6, 7 = Disabled

A-MSDU
User Priority 1, 2 = Enabled
User Priority 0, 3, 4, 5, 6, 7 = Disabled

In the 7.0.116.0 release for the Cisco Unified Wireless LAN Controller, the default A-MPDU and A-MSDU configuration is the following.

A-MPDU
User Priority 0, 4, 5 = Enabled
User Priority 1, 2, 3, 6, 7 = Disabled

A-MSDU
User Priority 0, 1, 2, 3, 4, 5 = Enabled
User Priority 6, 7 = Disabled

Use the following commands to configure the A-MPDU and A-MSDU settings per Cisco Cius recommendations.

In order to configure the 5 GHz settings, the 802.11a network will need to be disabled first, then re-enabled after the changes are complete.

```
config 802.11a 11nSupport a-mpdu tx priority 0 enable
config 802.11a 11nSupport a-mpdu tx priority 3 enable
config 802.11a 11nSupport a-mpdu tx priority 4 enable
config 802.11a 11nSupport a-mpdu tx priority 5 enable
config 802.11a 11nSupport a-mpdu tx priority 1 disable
config 802.11a 11nSupport a-mpdu tx priority 2 disable
config 802.11a 11nSupport a-mpdu tx priority 6 disable
config 802.11a 11nSupport a-mpdu tx priority 7 disable
config 802.11a 11nSupport a-msdu tx priority 1 enable
config 802.11a 11nSupport a-msdu tx priority 2 enable
config 802.11a 11nSupport a-msdu tx priority 0 disable
config 802.11a 11nSupport a-msdu tx priority 3 disable
config 802.11a 11nSupport a-msdu tx priority 4 disable
config 802.11a 11nSupport a-msdu tx priority 5 disable
config 802.11a 11nSupport a-msdu tx priority 6 disable
config 802.11a 11nSupport a-msdu tx priority 7 disable
```

In order to configure the 2.4 GHz settings, the 802.11b/g network will need to be disabled first, then re-enabled after the changes are complete.

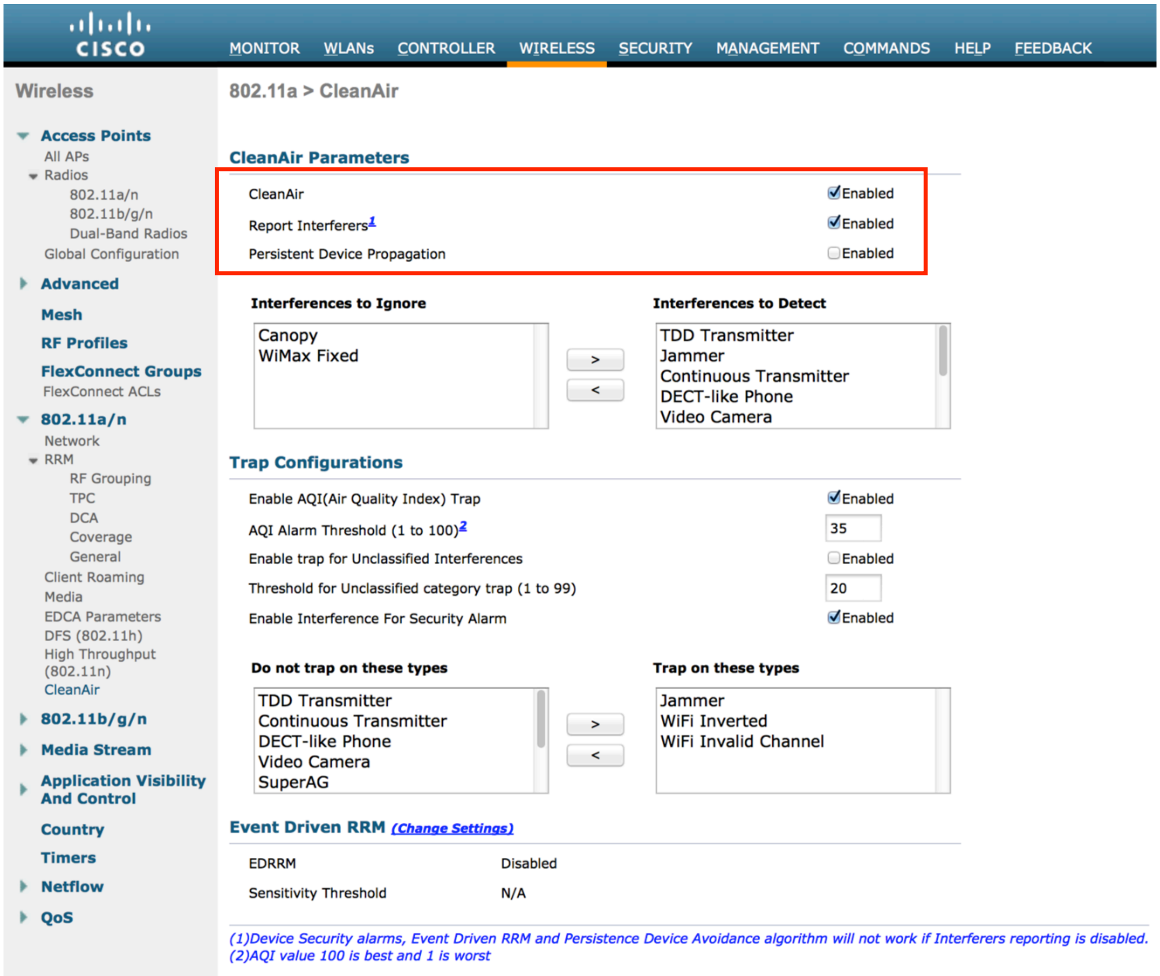
```
config 802.11b 11nSupport a-mpdu tx priority 0 enable
config 802.11b 11nSupport a-mpdu tx priority 3 enable
config 802.11b 11nSupport a-mpdu tx priority 4 enable
config 802.11b 11nSupport a-mpdu tx priority 5 enable
config 802.11b 11nSupport a-mpdu tx priority 1 disable
config 802.11b 11nSupport a-mpdu tx priority 2 disable
config 802.11b 11nSupport a-mpdu tx priority 6 disable
config 802.11b 11nSupport a-mpdu tx priority 7 disable
config 802.11b 11nSupport a-msdu tx priority 1 enable
config 802.11b 11nSupport a-msdu tx priority 2 enable
config 802.11b 11nSupport a-msdu tx priority 0 disable
config 802.11b 11nSupport a-msdu tx priority 3 disable
config 802.11b 11nSupport a-msdu tx priority 4 disable
config 802.11b 11nSupport a-msdu tx priority 5 disable
config 802.11b 11nSupport a-msdu tx priority 6 disable
config 802.11b 11nSupport a-msdu tx priority 7 disable
```

To view the current A-MPDU and A-MSDU configuration, enter either **show 802.11a** for 5 GHz or **show 802.11b** for 2.4 GHz.

```
802.11n Status:
  A-MPDU Tx:
    Priority 0............................... Enabled
    Priority 1............................... Disabled
    Priority 2............................... Disabled
    Priority 3............................... Enabled
    Priority 4.............................. Enabled
    Priority 5.............................. Enabled
    Priority 6.............................. Disabled
    Priority 7.............................. Disabled
  A-MSDU Tx:
    Priority 0.............................. Disabled
    Priority 1.............................. Enabled
    Priority 2.............................. Enabled
    Priority 3.............................. Disabled
    Priority 4.............................. Disabled
    Priority 5.............................. Disabled
    Priority 6.............................. Disabled
    Priority 7.............................. Disabled
```

CleanAir

CleanAir should be **Enabled** when utilizing Cisco Access Points with CleanAir technology in order to detect any existing interferers.



802.11a > CleanAir

CleanAir Parameters

CleanAir	☑ Enabled
Report Interferers[1]	☑ Enabled
Persistent Device Propagation	□ Enabled

Interferences to Ignore	Interferences to Detect
Canopy WiMax Fixed	TDD Transmitter Jammer Continuous Transmitter DECT-like Phone Video Camera

Trap Configurations

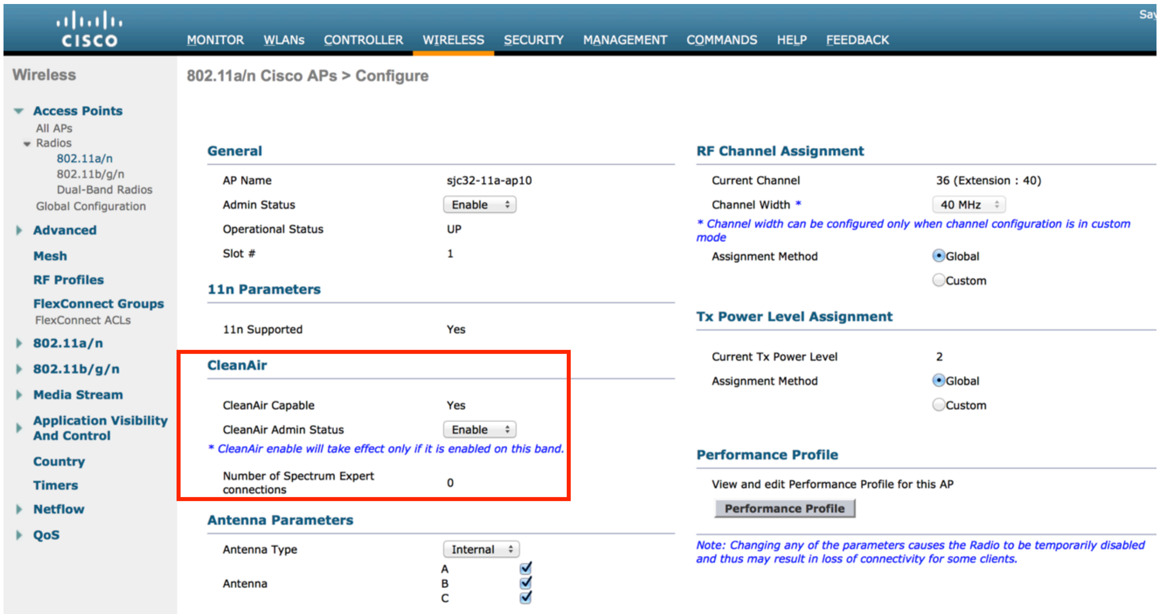
Enable AQI(Air Quality Index) Trap	☑ Enabled
AQI Alarm Threshold (1 to 100)[2]	35
Enable trap for Unclassified Interferences	□ Enabled
Threshold for Unclassified category trap (1 to 99)	20
Enable Interference For Security Alarm	☑ Enabled

Do not trap on these types	Trap on these types
TDD Transmitter Continuous Transmitter DECT-like Phone Video Camera SuperAG	Jammer WiFi Inverted WiFi Invalid Channel

Event Driven RRM *(Change Settings)*

EDRRM	Disabled
Sensitivity Threshold	N/A

(1)Device Security alarms, Event Driven RRM and Persistence Device Avoidance algorithm will not work if Interferers reporting is disabled.
(2)AQI value 100 is best and 1 is worst



802.11a/n Cisco APs > Configure

General

AP Name	sjc32-11a-ap10
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

CleanAir

CleanAir Capable	Yes
CleanAir Admin Status	Enable

** CleanAir enable will take effect only if it is enabled on this band.*

Number of Spectrum Expert connections	0

Antenna Parameters

Antenna Type	Internal
Antenna	A ☑ B ☑ C ☑

RF Channel Assignment

Current Channel	36 (Extension : 40)
Channel Width *	40 MHz

** Channel width can be configured only when channel configuration is in custom mode*

Assignment Method	● Global ○ Custom

Tx Power Level Assignment

Current Tx Power Level	2
Assignment Method	● Global ○ Custom

Performance Profile

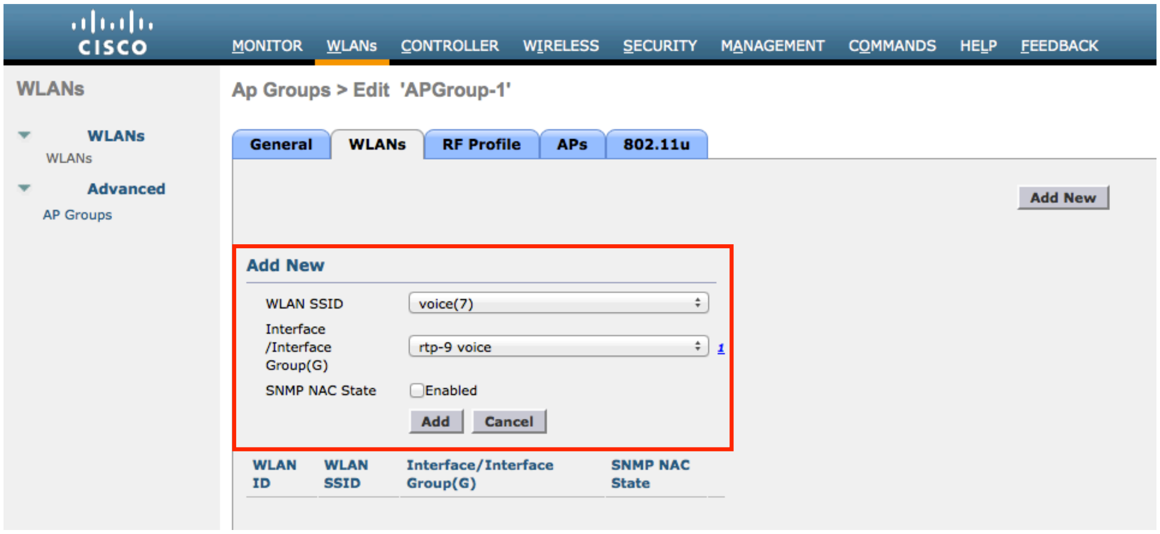
View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

AP Groups

AP Groups can be created to specify which WLANs / SSIDs are to be enabled and which interface they should be mapped to as well as what RF Profile parameters should be used for the access points assigned to the AP Group.

On the **WLANs** tab, select the desired SSIDs and interfaces to map to then select **Add**.



Ap Groups > Edit 'APGroup-1'

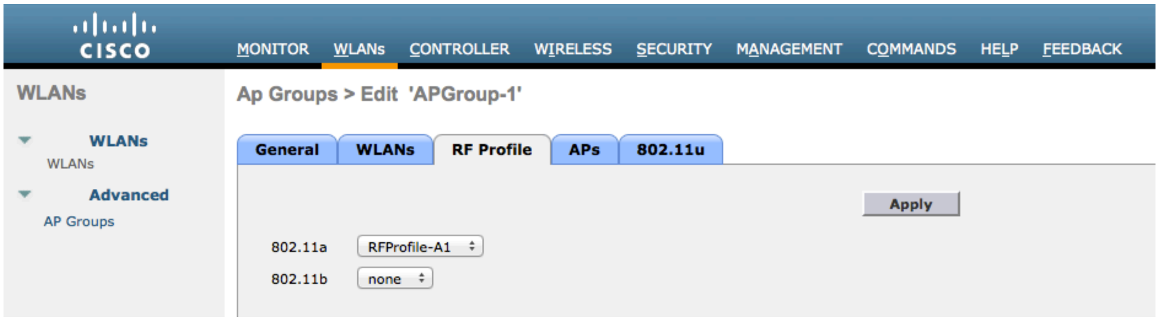
Add New

WLAN SSID	voice(7)
Interface /Interface Group(G)	rtp-9 voice
SNMP NAC State	□ Enabled

WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State

On the **RF Profile** tab, select the desired 802.11a or 802.11b RF Profile, then select **Apply**.

If changes are made after access points have joined the AP Group, then those access points will reboot once those changes are made



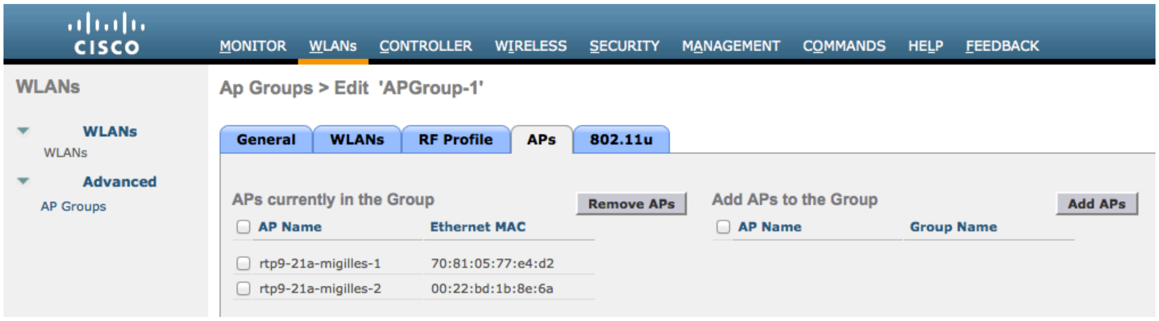
Ap Groups > Edit 'APGroup-1'

802.11a RFProfile-A1

802.11b none

On the **APs** tab, select the desired access points then select **Add APs**.

Those access points will then reboot.



Ap Groups > Edit 'APGroup-1'

APs currently in the Group

□	AP Name	Ethernet MAC
□	rtp9-21a-migilles-1	70:81:05:77:e4:d2
□	rtp9-21a-migilles-2	00:22:bd:1b:8e:6a

Add APs to the Group

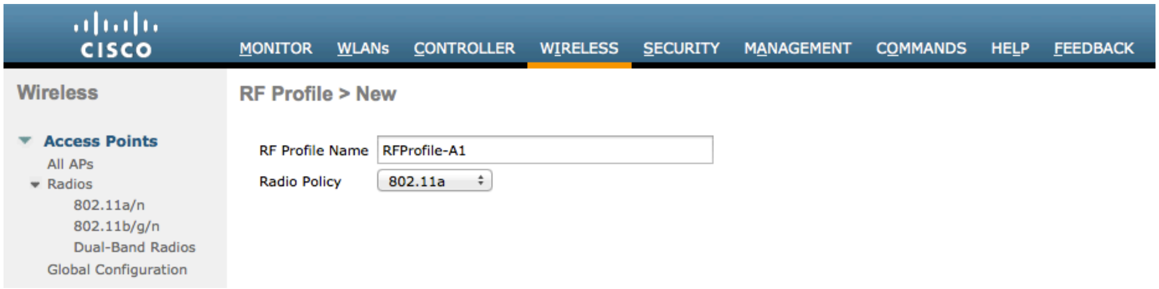
□	AP Name	Group Name

RF Profiles

RF Profiles can be created to specify which frequency bands, data rates, RRM settings, etc. a group of access points should use. RF Profiles are applied to an AP group once created. See the AP Groups section for more info on AP Group configuration.

When creating an RF Profile, the **RF Profile Name** and **Radio Policy** must be defined.

Select 802.11a or 802.11b/g for the **Radio Policy**.



RF Profile > New

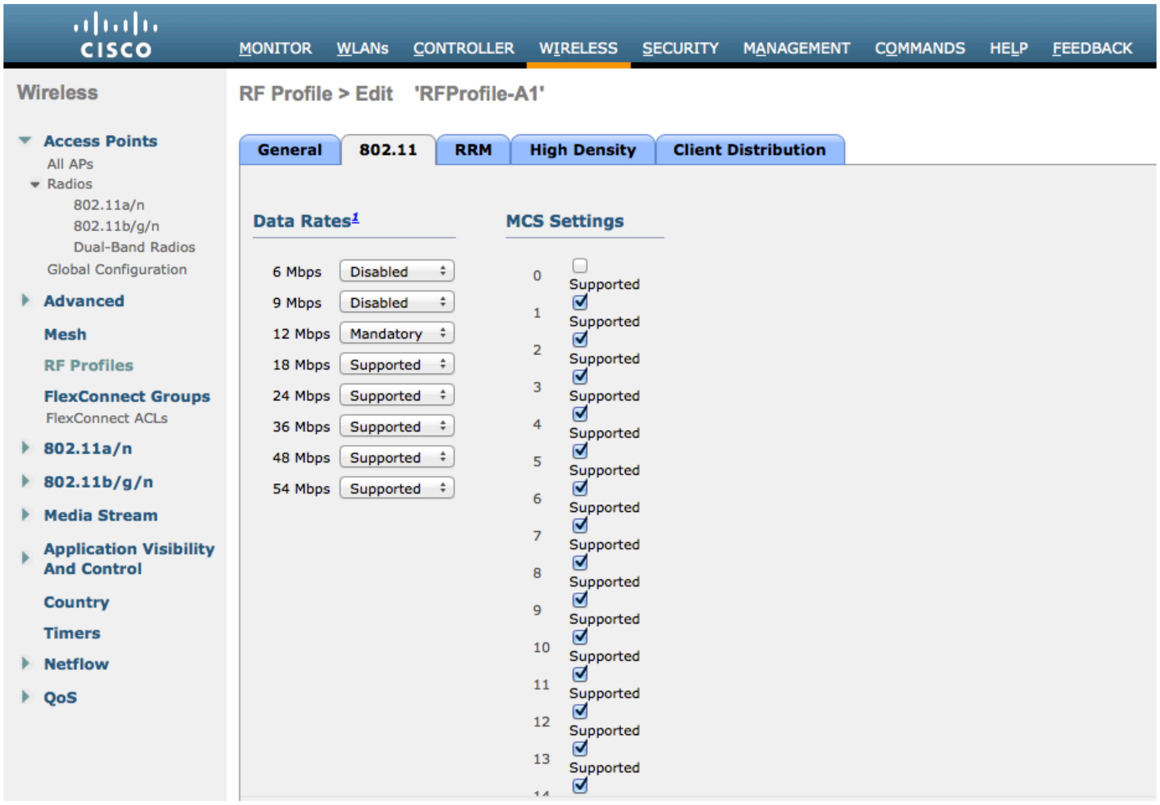
RF Profile Name RFProfile-A1

Radio Policy 802.11a

On the **802.11** tab, configure the data rates as desired.

Is recommended to enable 12 Mbps as **Mandatory** and 18-54 Mbps as **Supported**; however some environments may require 6 Mbps to be enabled as a mandatory (basic) rate.

MCS 0 should be disabled unless 6 Mbps is also enabled.



RF Profile > Edit 'RFProfile-A1'

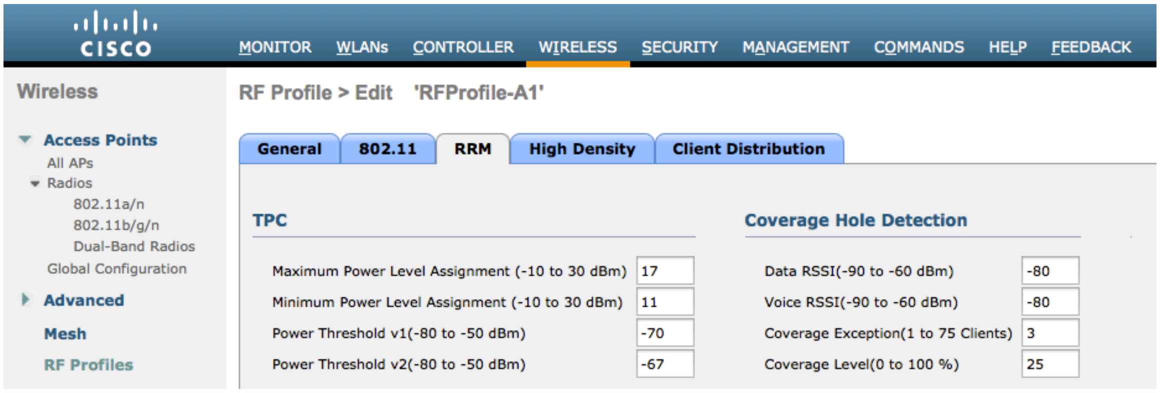
Data Rates[1]

6 Mbps	Disabled
9 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

MCS Settings

0	□ Supported
1	☑ Supported
2	☑ Supported
3	☑ Supported
4	☑ Supported
5	☑ Supported
6	☑ Supported
7	☑ Supported
8	☑ Supported
9	☑ Supported
10	☑ Supported
11	☑ Supported
12	☑ Supported
13	☑ Supported
14	☑

On the RRM tab, the **Maximum Power Level Assignment** and **Minimum Power Level Assignment** settings as well as other **TPC** and **Coverage Hole Detection** settings can be configured.


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
RF Profiles
General 802.11 RRM High Density Client Distribution

RF Profile > Edit 'RFProfile-A1'

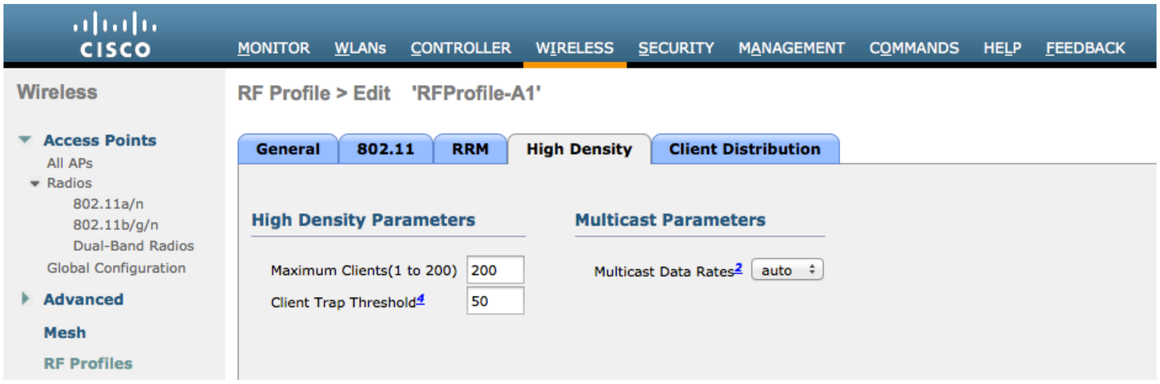
TPC

Maximum Power Level Assignment (-10 to 30 dBm)	17
Minimum Power Level Assignment (-10 to 30 dBm)	11
Power Threshold v1(-80 to -50 dBm)	-70
Power Threshold v2(-80 to -50 dBm)	-67

Coverage Hole Detection

Data RSSI(-90 to -60 dBm)	-80
Voice RSSI(-90 to -60 dBm)	-80
Coverage Exception(1 to 75 Clients)	3
Coverage Level(0 to 100 %)	25

On the High Density tab, Maximum Clients and Multicast Data Rates can be configured.



RF Profile > Edit 'RFProfile-A1'

High Density Parameters

Maximum Clients(1 to 200) 200

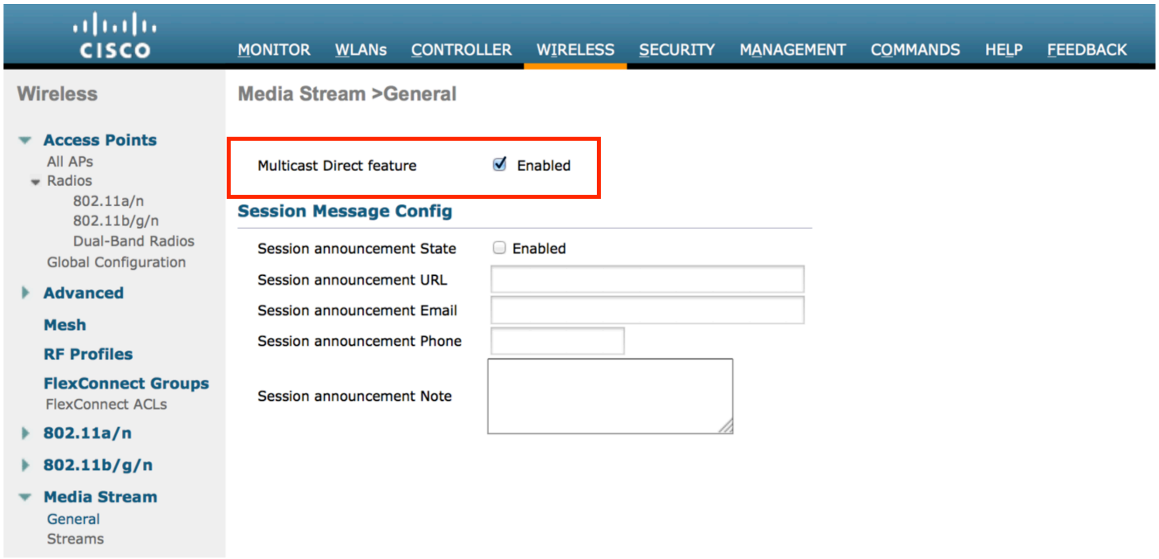
Client Trap Threshold[4] 50

Multicast Parameters

Multicast Data Rates[2] auto

Multicast Direct

In the Media Stream settings, **Multicast Direct feature** should be enabled.



Media Stream >General

Multicast Direct feature ☑ Enabled

Session Message Config

Session announcement State ☐ Enabled

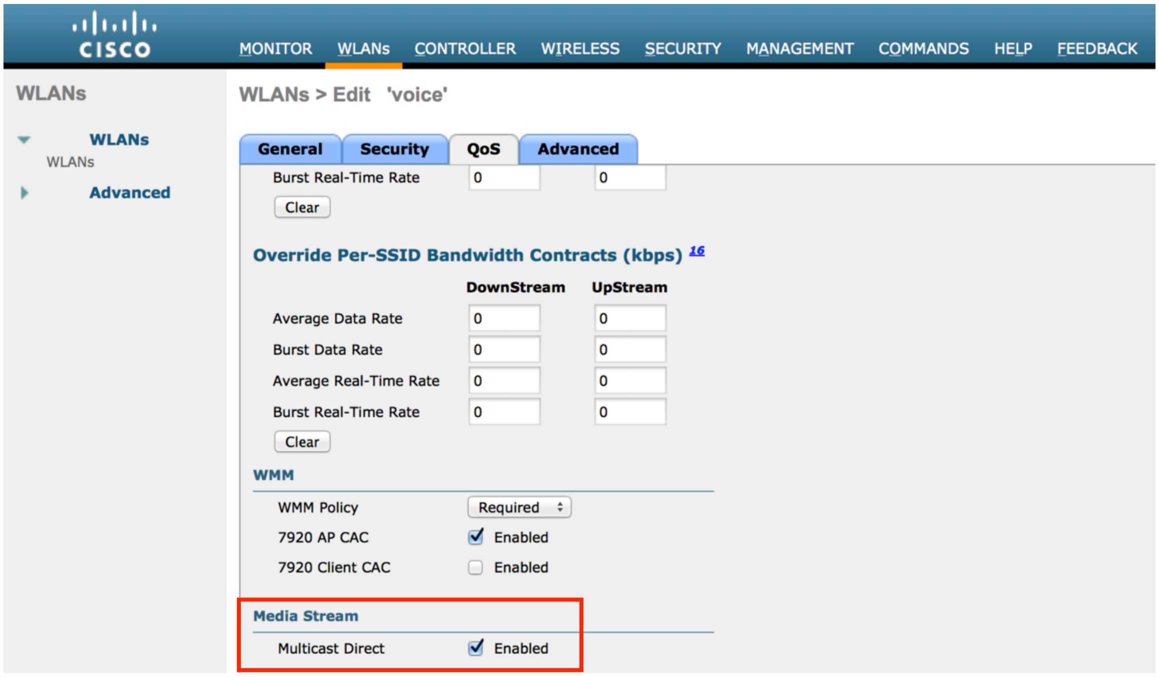
Session announcement URL

Session announcement Email

Session announcement Phone

Session announcement Note

After **Multicast Direct feature** is enabled, then there will be an option to enable **Multicast Direct** in the QoS menu of the WLAN configuration.



WLANs > Edit 'voice'

Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) [16]

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WMM

WMM Policy: Required

7920 AP CAC ☑ Enabled

7920 Client CAC □ Enabled

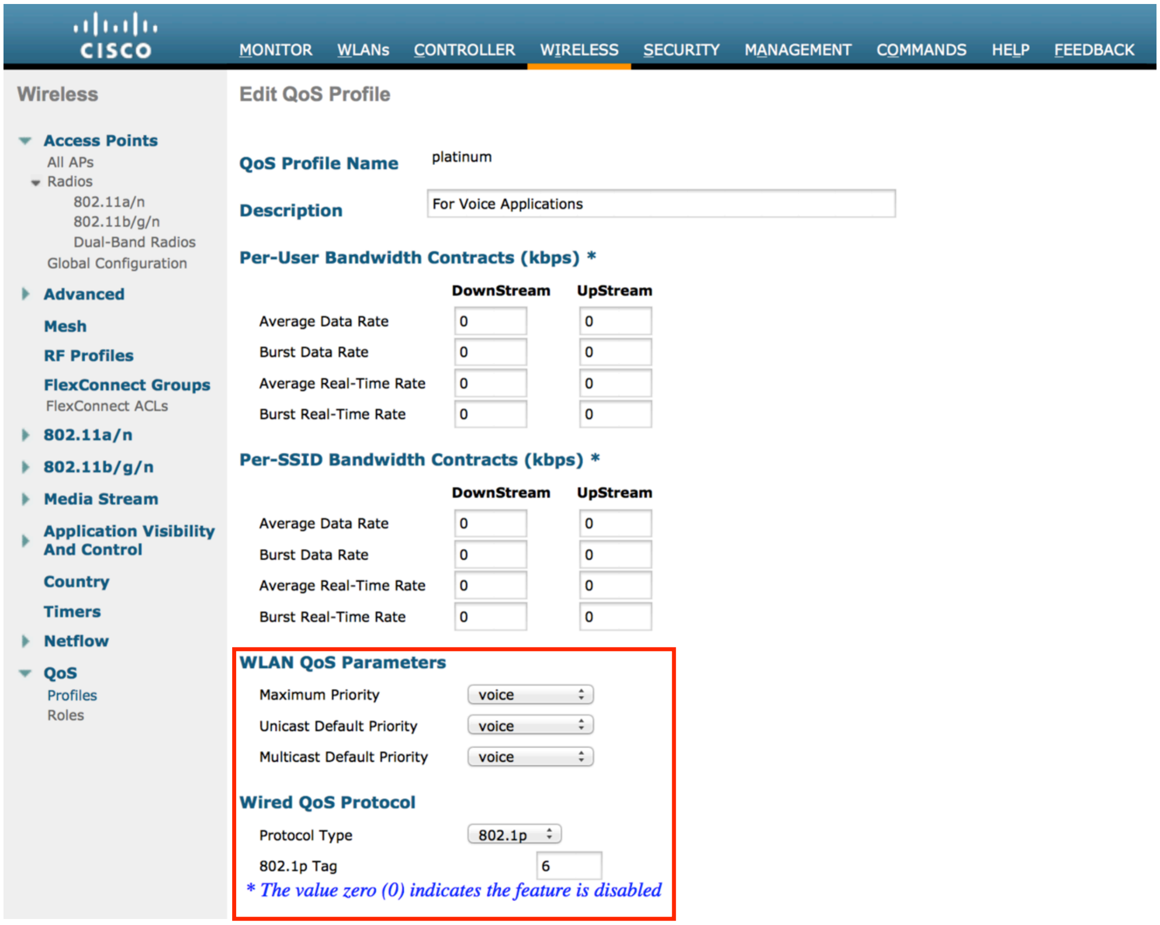
Media Stream

Multicast Direct ☑ Enabled

QoS Profiles

Configure the four QoS profiles (Platinum, Gold, Silver, Bronze), by selecting **802.1p** as the protocol type and set the **802.1p tag** for each profile.

- Platinum =6
- Gold = 5
- Silver = 3
- Bronze = 1



Edit QoS Profile

QoS Profile Name: platinum

Description: For Voice Applications

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority: voice

Unicast Default Priority: voice

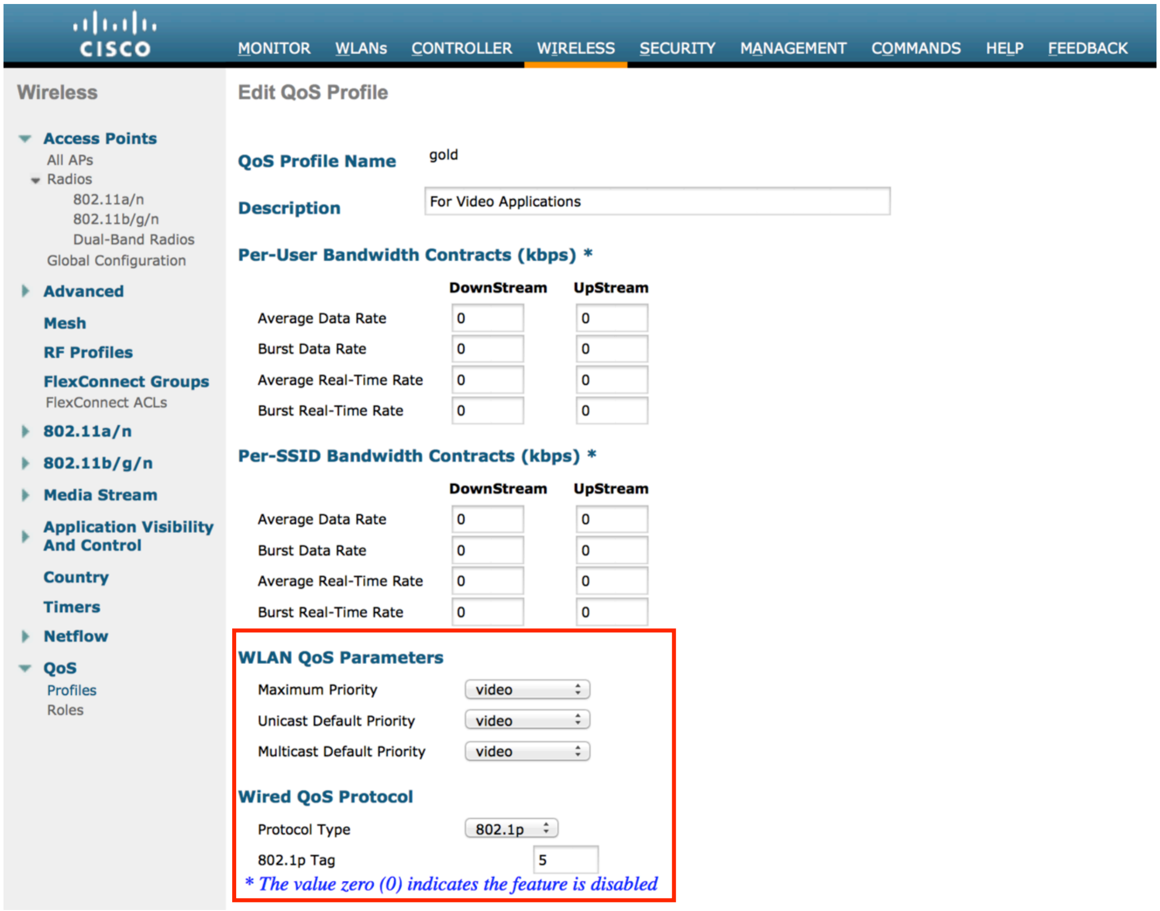
Multicast Default Priority: voice

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 6

* *The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name: gold

Description: For Video Applications

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority: video

Unicast Default Priority: video

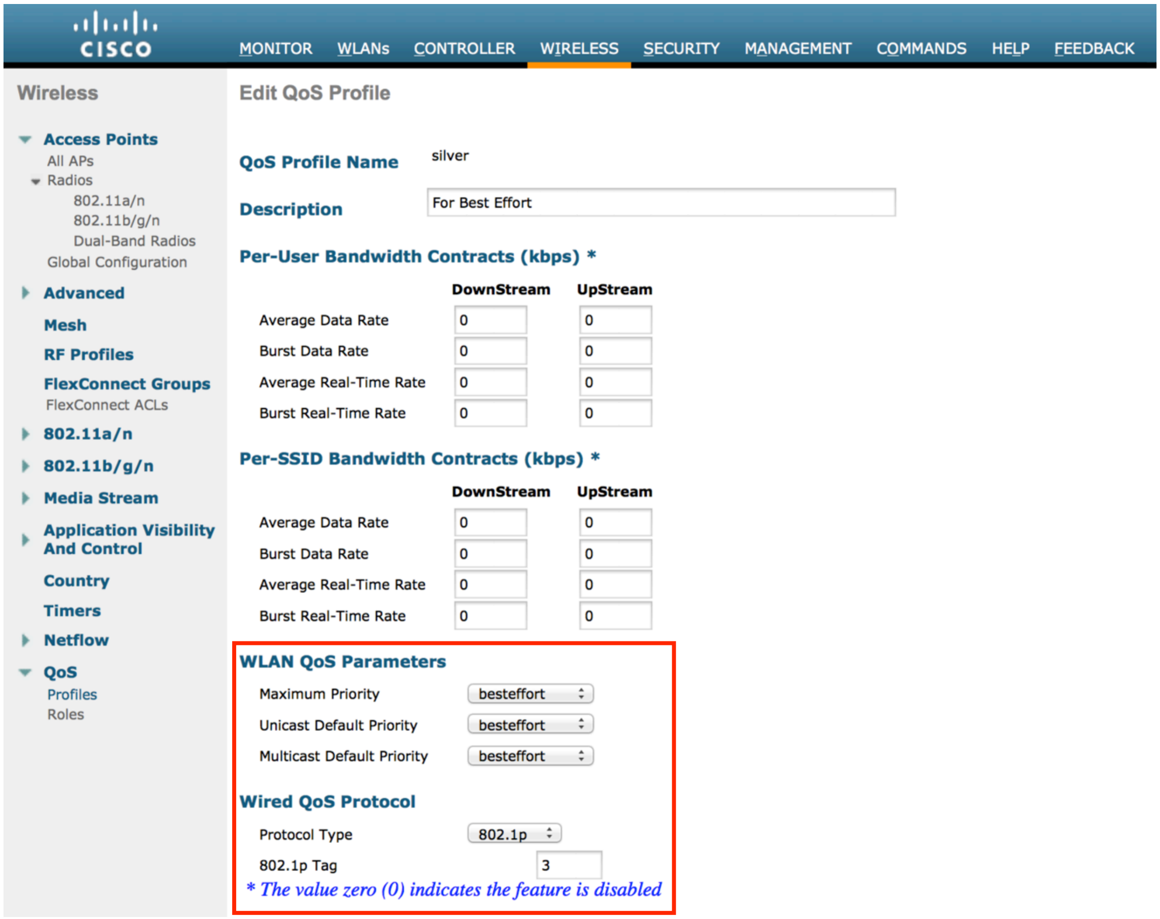
Multicast Default Priority: video

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 5

* *The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name: silver

Description: For Best Effort

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority: besteffort

Unicast Default Priority: besteffort

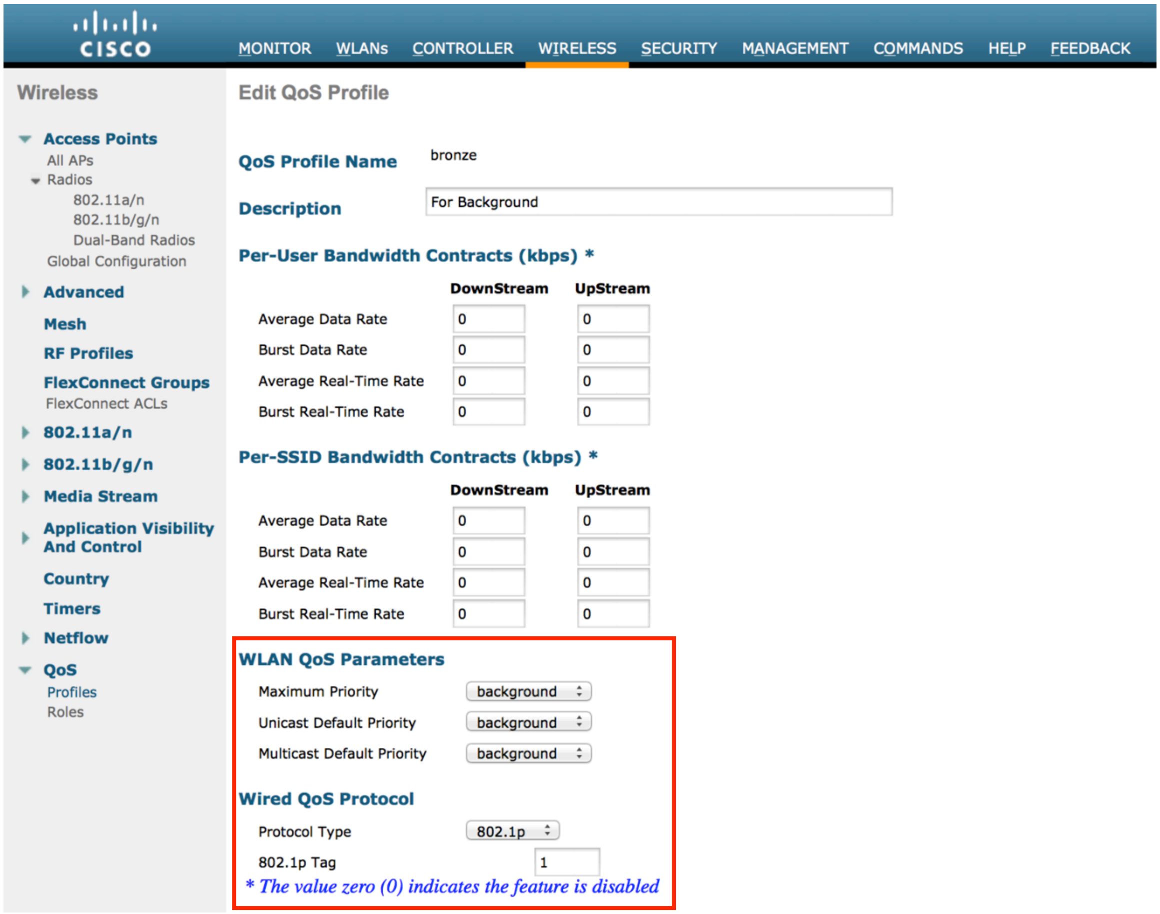
Multicast Default Priority: besteffort

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 3

** The value zero (0) indicates the feature is disabled*



Edit QoS Profile

QoS Profile Name: bronze

Description: For Background

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

WLAN QoS Parameters

Maximum Priority: background

Unicast Default Priority: background

Multicast Default Priority: background

Wired QoS Protocol

Protocol Type: 802.1p

802.1p Tag: 1

** The value zero (0) indicates the feature is disabled*

QoS Basic Service Set (QBSS)

There are three different versions of QoS Basic Service Set (QBSS) that Cisco Cius supports.

The first version from Cisco was on a 0-100 scale and was not based on clear channel assessment (CCA), so it does not account for channel utilization, but only the 802.11 traffic traversing that individual access point's radio. So it does not account for other 802.11 energy or interferers using the same frequencies. The max threshold is defined on the client side, which is set to 45.

QBSS is also a part of 802.11e, which is on a 0-255 scale and is CCA based. So this gives a true representation on how busy the channel is. The max threshold is also defined on the client side, which is set to 105.

Cisco Cius converts the QBSS info to a percentage format (0-255 to 0-100%), which is displayed as the Channel Utilization value in the neighbor list menu.

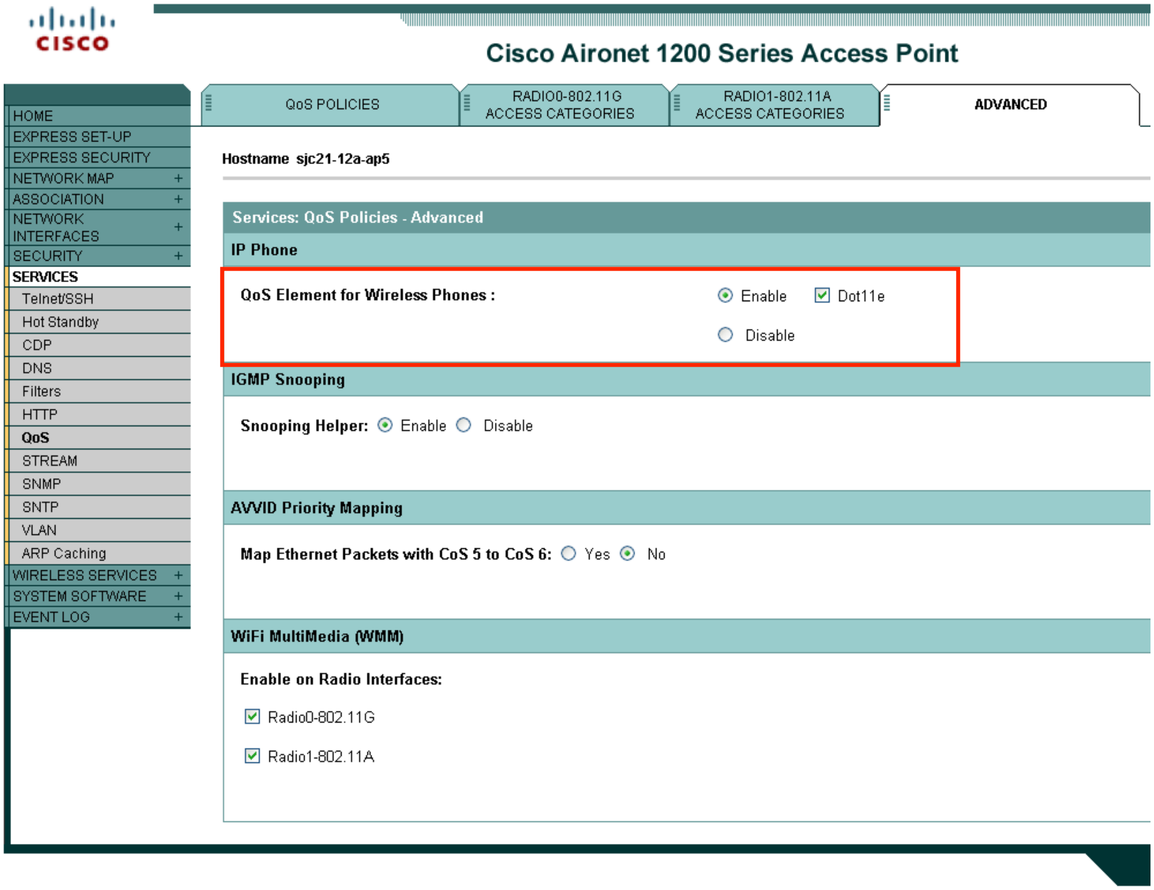
The second version from Cisco is based on the 802.11e version, but allows the default max threshold of 105 to be optionally configured.

Each version of QBSS can be optionally be configured on the access point.

For the Cisco Unified Wireless LAN Controller, enabling WMM will enable the 802.11e version of QBSS. There are also the **7920 Client CAC** and **7920 AP CAC** options, where **7920 Client CAC** will enable Cisco version 1 and **7920 AP CAC** enables Cisco version 2. See the SSID / WLAN QoS Settings section for more info.

For the Cisco Autonomous Access Point, **dot11 phone** or **dot11 phone dot11e** will enable QBSS.

Dot11 phone will enable the 2 Cisco versions, where **dot11 phone dot11e** will enable both CCA versions (802.11e and Cisco version 2). It is recommended to enable **dot11 phone dot11e**.



Hostname sjc21-12a-ap5

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:

☑ Radio0-802.11G

☑ Radio1-802.11A

CCKM Timestamp Tolerance

As of the 7.0.98.218 release, the CCKM timestamp tolerance is configurable.

In previous releases, the CCKM timestamp tolerance was set to 1000 ms and non-configurable.

The default CCKM timestamp tolerance is still set to 1000 ms in the later releases.

It is recommended to adjust the CCKM timestamp tolerance to 5000 ms to optimize the Cisco Cius roaming experience.

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance ?
 <tolerance>    Allow CCKM IE time-stamp tolerance <1000 to 5000> milliseconds; Default tolerance 1000 msecs
```

Use the following command to configure the CCKM timestamp tolerance per Cisco recommendations.

```
(Cisco Controller) >config wlan security wpa akm cckm timestamp-tolerance 5000 <WLAN id >
```

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

```
CCKM tsf Tolerance.............................. 5000
```

Auto-Immune

The Auto-Immune feature can optionally be enabled for protection against denial of service (DoS) attacks.

Although when this feature is enabled there can be interruptions introduced with voice over wireless LAN, therefore it is recommended to disable the Auto-Immune feature on the Cisco Unified Wireless LAN Controller.

To view the Auto-Immune configuration on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >show wps summary

Auto-Immune
  Auto-Immune.................................. Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft..................................... Enabled
  Excessive Web authentication failure........... Enabled

Signature Policy
  Signature Processing.......................... Enabled
```

To disable the Auto-Immune feature on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config wps auto-immune disable
```

WLAN Controller Advanced EAP Settings

Need to ensure that the advanced EAP settings in the Cisco Unified Wireless LAN Controller are configured per the information below.

To view the EAP configuration on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >show advanced eap
        EAP-Identity-Request Timeout (seconds)........... 30
        EAP-Identity-Request Max Retries................. 2
        EAP Key-Index for Dynamic WEP.................... 0
        EAP Max-Login Ignore Identity Response........... enable
        EAP-Request Timeout (seconds).................... 30
        EAP-Request Max Retries.......................... 2
        EAPOL-Key Timeout (milliseconds)...................... 400
        EAPOL-Key Max Retries............................ 4
```

If using 802.1x or WPA/WPA2, the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller should be set to at least 20 seconds.

In later versions of Cisco Unified Wireless LAN Controller software, the default EAP-Request Timeout was changed from 2 to 30 seconds.

The default timeout on the Cisco ACS server is 20 seconds.

To change the EAP-Request Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap request-timeout 30
```

If using WPA/WPA2 PSK then it is recommended to reduce the EAPOL-Key Timeout to 400 milliseconds from the default of 1000 milliseconds with EAPOL-Key Max Retries set to 4 from the default of 2.

If using WPA/WPA2, then using the default values where the EAPOL-Key Timeout is set to 1000 milliseconds and EAPOL-Key Max Retries are set to 2 should work fine, but is still recommended to set those values to 400 and 4 respectively.

The EAPOL-Key Timeout should not exceed 1 second (1000 milliseconds).

To change the EAPOL-Key Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap eapol-key-timeout 400
```

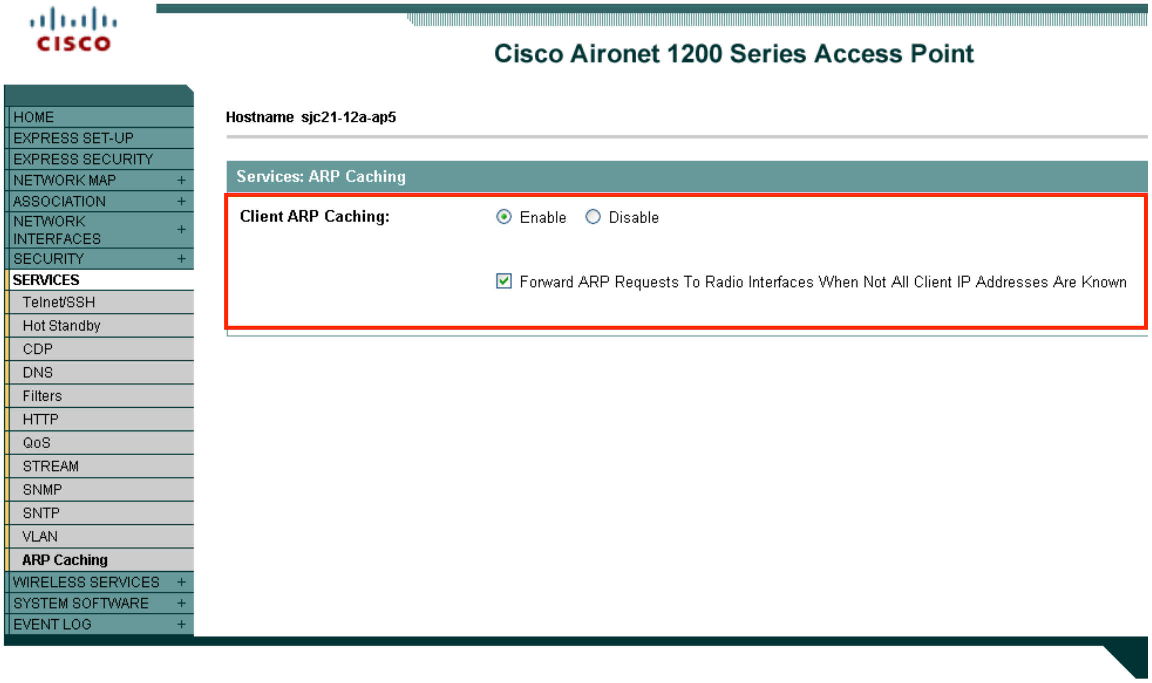
To change the EAPOL-Key Max Retries Timeout on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command.

```
(Cisco Controller) >config advanced eap eapol-key-retries 4
```

Proxy ARP

To advertise the proxy ARP information element, ensure that **Aironet Extensions** are enabled.

For Cisco Autonomous Access Points, enter **dot11 arp-cache optional**.



Cisco Aironet 1200 Series Access Point

Hostname sjc21-12a-ap5

Services: ARP Caching

Client ARP Caching: ● Enable ○ Disable

☑ Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known

TKIP Countermeasure Holdoff Time

TKIP countermeasure mode can occur if the access point receives two message integrity check (MIC) errors within a 60 second period. When this occurs, the access point will de-authenticate all TKIP clients associated to that 802.11 radio and holdoff any clients for the countermeasure holdoff time (default = 60 seconds).

To change the TKIP countermeasure holdoff time on the Cisco Unified Wireless LAN Controller, telnet or SSH to the controller and enter the following command:

```
(Cisco Controller) >config wlan security tkip hold-down <nseconds> <WLAN id>
```

To confirm the change, enter **show wlan <WLAN id>**, where the following will be displayed.

```
Tkip MIC Countermeasure Hold-down Timer....... 60
```

For the Cisco Autonomous Access Point, enter the time in seconds to holdoff clients if a TKIP countermeasure event occurs.

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

VLANs and Cisco Autonomous Access Points

Segment wireless voice and data into separate VLANs.

A subnet for wireless clients should not exceed 1,000 hosts.

When using Cisco Autonomous Access Points, use a dedicated native VLAN. The Cisco Autonomous Access Points utilize Inter-Access Point Protocol (IAPP), which is a multicast protocol.

For the native VLAN, it is recommended not to use VLAN 1 to ensure that IAPP packets are exchanged successfully.

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

Port security should be disabled on switch ports that Cisco Autonomous Access Points are directly connected to.

The network ID in the SSID configuration with the Cisco Autonomous Access Point should only be disabled if Layer 3 mobility is enabled where the Wireless LAN Services Module (WLSM) is deployed.

Configuring Cisco Cius

To configure the Wi-Fi settings on Cisco Cius, use the keypad and touch screen to navigate to **Settings > Wireless & networks > Wi-Fi settings.**

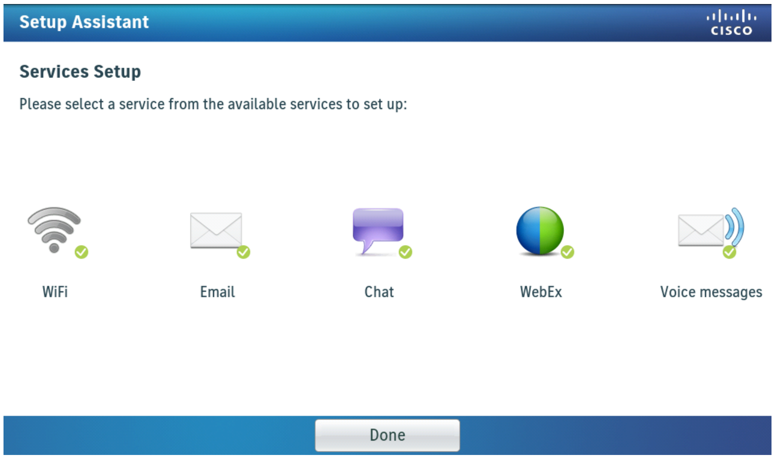
Setup Assistant

When first powering on Cisco Cius, the Setup Assistant will be launched to help guide the user through the services configuration.

Select the service to start the configuration process.

- WiFi
- Email
- Chat
- WebEx
- Voice Messages

A checkmark will be displayed when the service has been successfully configured.



Setup Assistant

Services Setup

Please select a service from the available services to set up:

Wireless LAN Settings

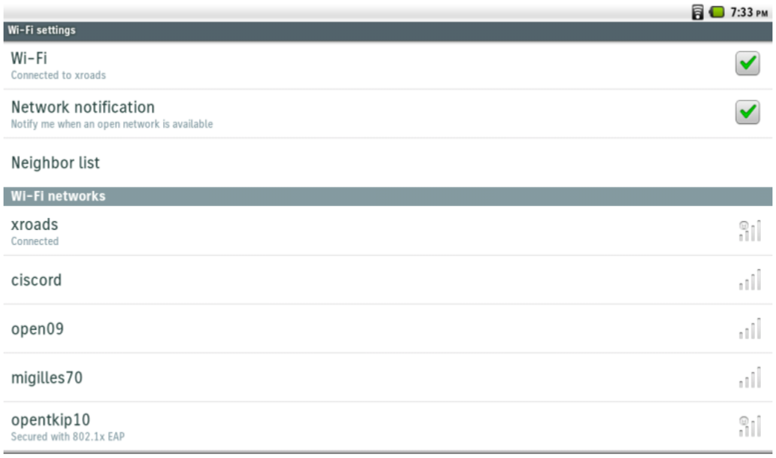
Use the following guidelines to configure the wireless LAN profile.

Cisco Cius can remember up to 8 wireless LANs profiles.

If unable to add a network, check to see if the max number of wireless LAN profiles has been met already, where one of those wireless LAN profiles may need to be deleted manually in order to add a new network.

- Navigate to **Settings > Wireless & networks > Wi-Fi**.
- Ensure that **Wi-Fi** is checked indicating that is enabled.

  Ensure **Wi-Fi** is enabled in the Cisco Unified Communications Manager; otherwise the option will be greyed out.
- Either select the broadcasted Wi-Fi network from the list or add the Wi-Fi network manually.
- If adding manually, enter the **SSID** (case sensitive).



Wi-Fi settings

Wi-Fi ☑
Connected to xroads

Network notification ☑
Notify me when an open network is available

Neighbor list

Wi-Fi networks

xroads
Connected

ciscord

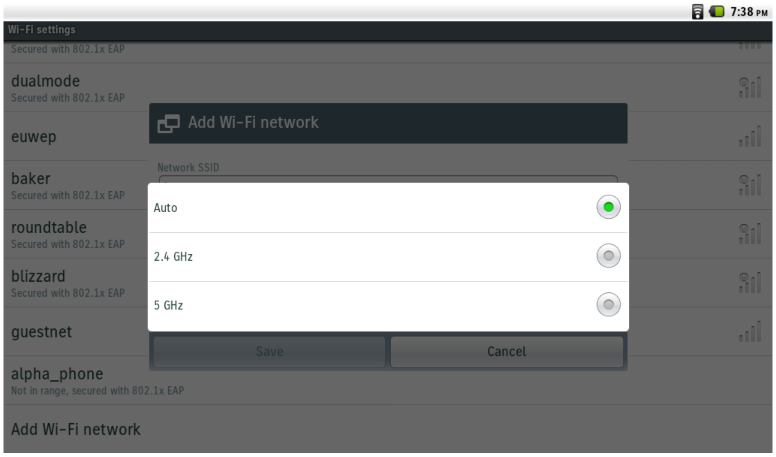
open09

migilles70

opentkip10
Secured with 802.1x EAP

- Select one of the following different 802.11 modes to set the frequency band.
  - Auto
  - 5 GHz
  - 2.4 GHz

(Auto mode will scan both 2.4 GHz and 5 GHz channels and attempt to associate to the access point with the strongest signal)



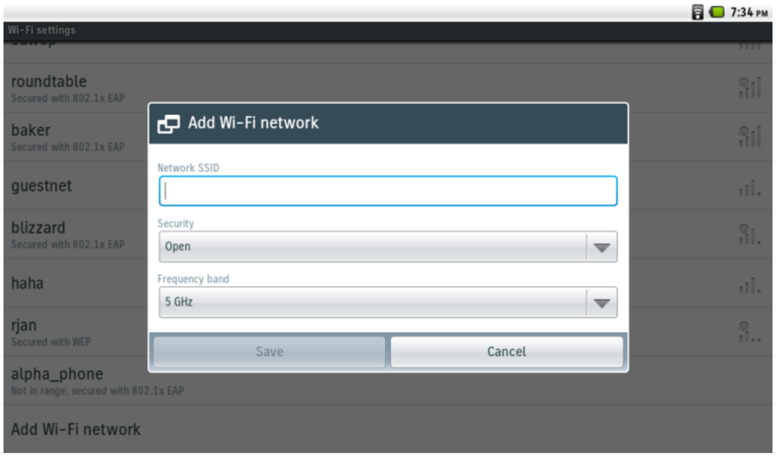
Auto ●
2.4 GHz ○
5 GHz ○

- Below lists the available security modes supported and the key management and encryption types that can be used for each mode.

  The key management and encryption type (cipher) will be auto-configured based on the access point’s current configuration, where precedence is giving to the strongest key management type enabled (e.g. WPA2) then the strongest cipher enabled (e.g. AES).

Security Mode	802.1x Type	Key Management	Encryption
Open	N/A	None	None
WEP	N/A	Static	WEP (40/64 or 104/128 bit)
WPA/WPA2 PSK	N/A	WPA-PSK, WPA2-PSK	TKIP, AES
802.1x EAP	EAP-FAST, PEAP, TLS	WPA, WPA2	TKIP, AES

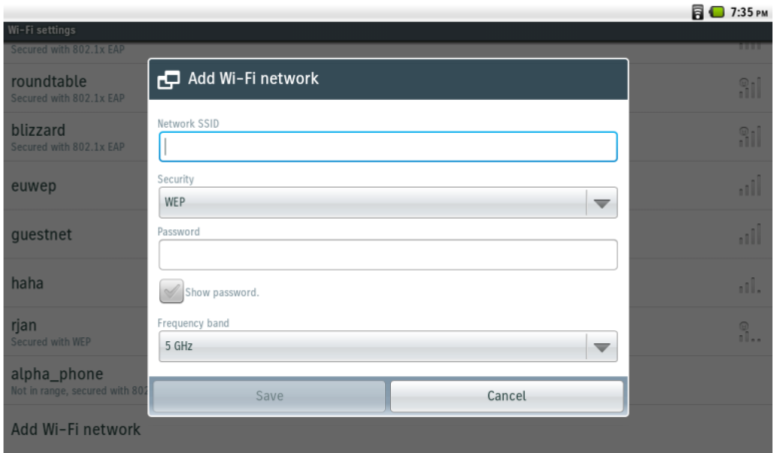
- If wanting to configure a wireless network profile without security (open security), then simply enter the **SSID** and select **Open** for the security type.



Network SSID:
Security: Open
Frequency band: 5 GHz

- **WEP** security mode requires that the static WEP key (password) be entered.
- Only key index 1 is supported, so will want to ensure that only key index 1 is configured on the access point.

Key Style	Key Size	Characters
ASCII	40/64 bit	5
ASCII	104/128 bit	13
HEX	40/64 bit	10 (0-9, A-F)
HEX	104/128 bit	26 (0-9, A-F)



Add Wi-Fi network

Network SSID

Security: WEP

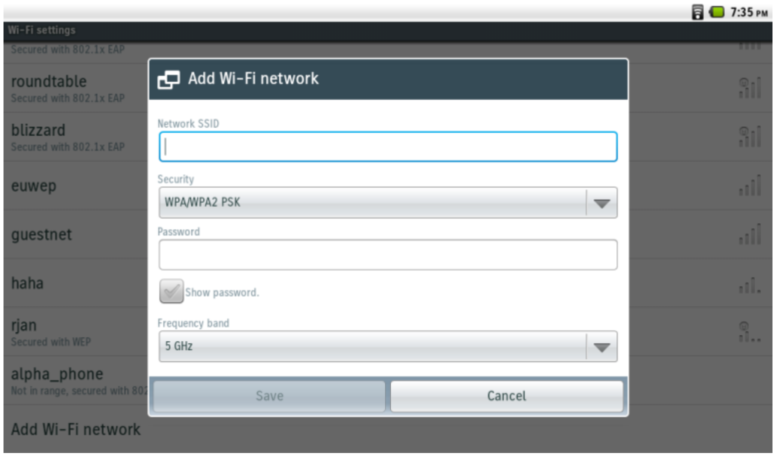
Password

☑ Show password.

Frequency band: 5 GHz

- If selecting **WPA/WPA2 PSK** as the security mode, then a Pre-Shared Key (password) must be configured.
- Enter the ASCII or hexadecimal formatted password.

Key Style	Characters
ASCII	8-63
HEX	64 (0-9,A-F)



Add Wi-Fi network

Network SSID

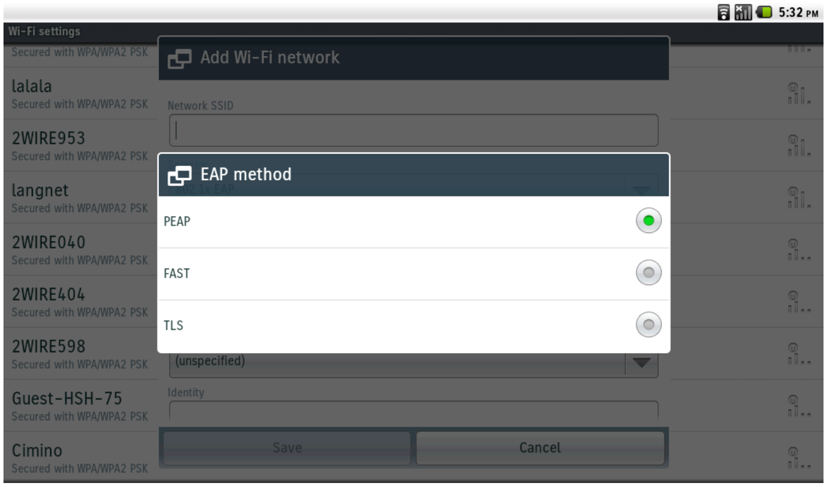
Security: WPA/WPA2 PSK

Password

☑ Show password.

Frequency band: 5 GHz

- If selecting **802.1x EAP** as the security mode, then a username (identity) and password must be configured if using EAP-FAST (FAST) or PEAP.
- If selecting PEAP, then the Phase 2 authentication type must be specified (MSCHAPv2 or GTC).
- A CA certificate can optionally be imported and configured if wanting to use PEAP with server validation.
- If using EAP-TLS (TLS), then a user certificate and CA certificate are required to be imported and configured.


Add Wi-Fi network

Network SSID

EAP method

PEAP ●

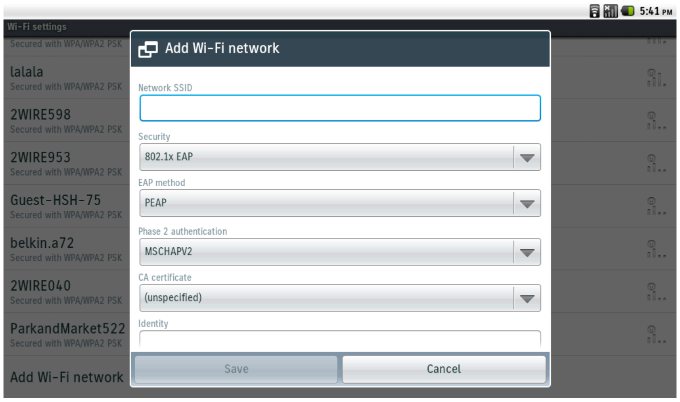
FAST ○

TLS ○

(unspecified)

Identity

Save | Cancel


Add Wi-Fi network

Network SSID

Security: 802.1x EAP

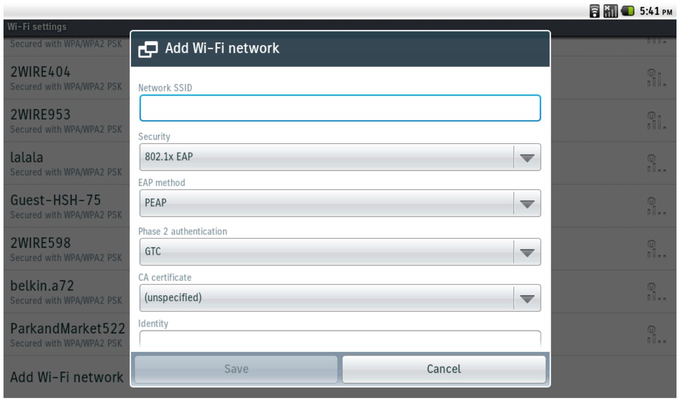
EAP method: PEAP

Phase 2 authentication: MSCHAPV2

CA certificate: (unspecified)

Identity

Save | Cancel


Add Wi-Fi network

Network SSID

Security: 802.1x EAP

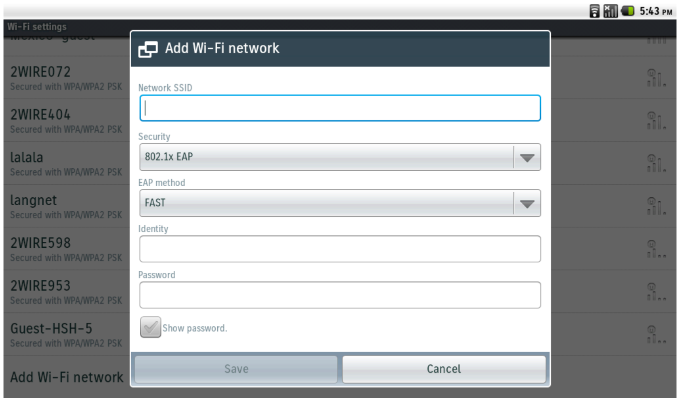
EAP method: PEAP

Phase 2 authentication: GTC

CA certificate: (unspecified)

Identity

Save | Cancel


Add Wi-Fi network

Network SSID

Security: 802.1x EAP

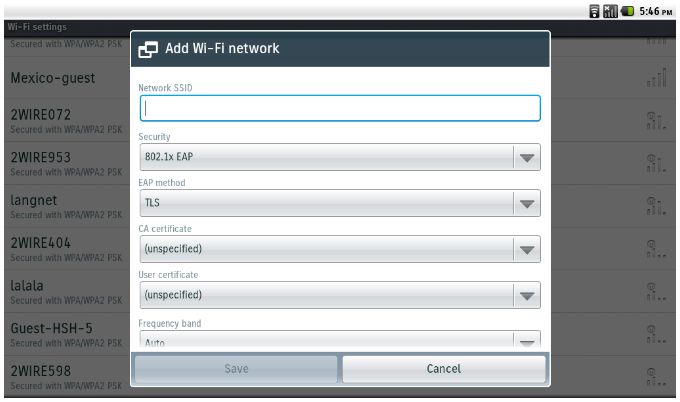
EAP method: FAST

Identity

Password

☑ Show password.

Save | Cancel


Add Wi-Fi network

Network SSID

Security: 802.1x EAP

EAP method: TLS

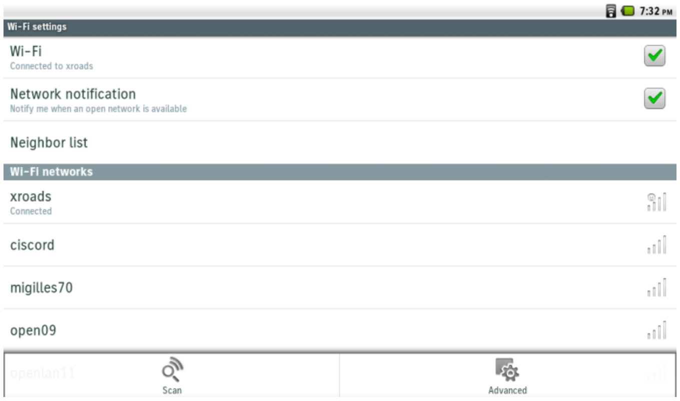
CA certificate: (unspecified)

User certificate: (unspecified)

Frequency band: Auto

Save | Cancel

- In the advanced menu of Wi-Fi settings, Dynamic Host Configuration Protocol (DHCP) or static IP settings can be configured. To access the advanced menu, select the menu hard button (far left) to display the **Advanced** menu option.


7:32 PM

Wi-Fi settings

Wi-Fi ☑
Connected to xroads

Network notification ☑
Notify me when an open network is available

Neighbor list

Wi-Fi networks

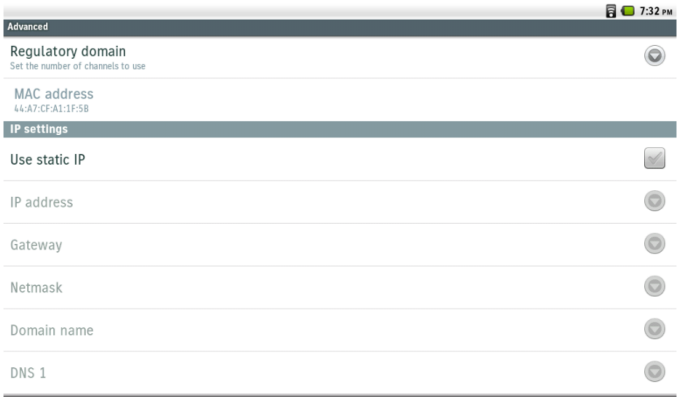
xroads
Connected

ciscord

migilles70

open09

openlan11


7:32 PM

Advanced

Regulatory domain
Set the number of channels to use

MAC address
44:A7:CF:A1:1F:5B

IP settings

Use static IP □

IP address

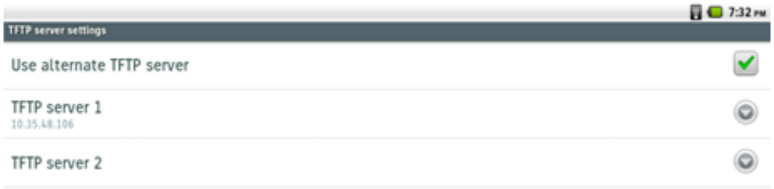
Gateway

Netmask

Domain name

DNS 1

- If DHCP option 150 or 66 is not configured to provide the TFTP server IP address via the network's DHCP scope, then enable **Use alternate TFTP server** in TFTP server settings and enter the IP address of the TFTP servers.


7:32 PM

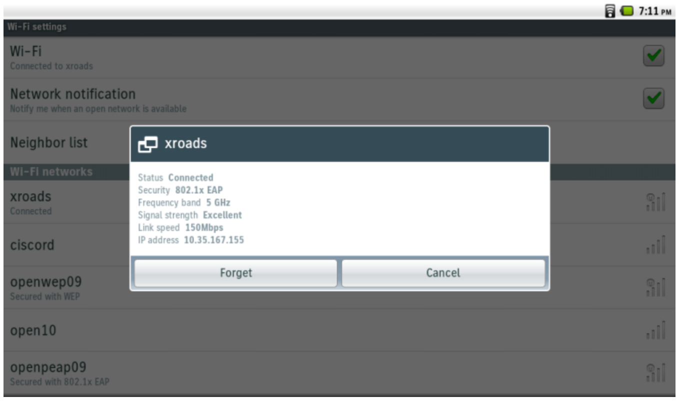
TFTP server settings

Use alternate TFTP server ☑

TFTP server 1
10.35.48.106

TFTP server 2

- Network profiles can be removed by tapping on the wireless LAN selection then selecting **Forget** or by selecting and holding the wireless LAN selection, where **Forget network** will be displayed.
- Wireless LAN profile parameters can be modified after selecting and holding the wireless LAN selection, then selecting **Modify network**.


7:11 PM

Wi-Fi settings

Wi-Fi ☑
Connected to xroads

Network notification ☑
Notify me when an open network is available

Neighbor list

Wi-Fi networks

xroads
Connected

ciscord

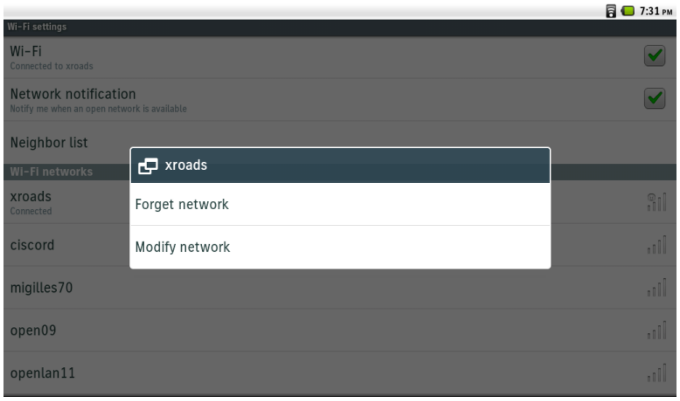
openwep09
Secured with WEP

open10

openpeap09
Secured with 802.1x EAP

xroads

Status Connected
Security 802.1x EAP
Frequency band 5 GHz
Signal strength Excellent
Link speed 150Mbps
IP address 10.35.167.155


7:31 PM

Wi-Fi settings

Wi-Fi ☑
Connected to xroads

Network notification ☑
Notify me when an open network is available

Neighbor list

Wi-Fi networks

xroads
Connected

ciscord

migilles70

open09

openlan11

xroads

Note: CCKM will be negotiated if enabled on the access point when using EAP-FAST, EAP-TLS or PEAP.

WEP128 is listed as WEP104 on the Cisco Unified Wireless LAN Controllers.

When Airplane mode is enabled, the Wi-Fi interface is disabled, but can be re-enabled optionally while still in Airplane mode.

Shared Key authentication and 802.1x + Dynamic WEP are not supported.

For more information, refer to the **Configuring Settings on Cisco Cius** in the Cisco Cius Administration Guide at this URL: http://www.cisco.com/en/US/products/ps11156/prod_maintenance_guides_list.html

Installing Certificates

Cisco Cius supports DER encoded binary X.509 certificates, which can be utilized with EAP-TLS or for authentication server validation when using PEAP.

Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is using the TLS protocol with PKI to secure communications to the authentication server.

TLS provides a way to use certificates for both user and server authentication and for dynamic session key generation.

EAP-TLS provides excellent security, but requires client certificate management.

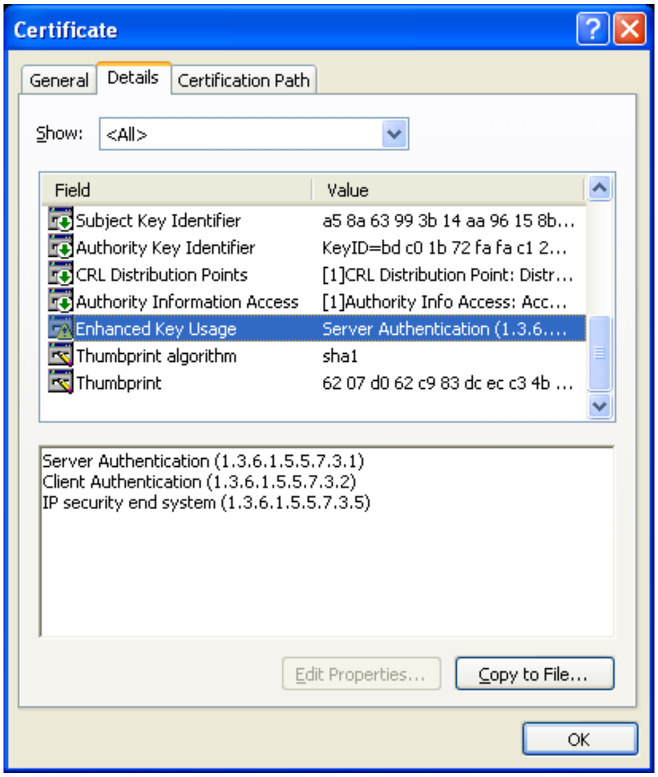
Microsoft® Certificate Authority (CA) servers are recommended as we have certified interoperability only with those CA types. Other CA server types may not be completely interoperable with Cisco Cius.

Both DER and Base-64 formats are acceptable for the client and server certificates.

Certificates with a key size of 1024, 2048, and 4096 are supported.

Ensure the client and server certificates are signed using either the SHA-1 or SHA-2 algorithm, as the SHA-3 signature algorithms are not supported.

Ensure Client Authentication is listed in the Enhanced Key Usage section of the user certificate details.



Show: <All>

Field	Value
Subject Key Identifier	a5 8a 63 99 3b 14 aa 96 15 8b...
Authority Key Identifier	KeyID=bd c0 1b 72 fa fa c1 2...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Server Authentication (1.3.6....
Thumbprint algorithm	sha1
Thumbprint	62 07 d0 62 c9 83 dc ec c3 4b ...

Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
IP security end system (1.3.6.1.5.5.7.3.5)

X.509 digital certificates are required to be installed if utilizing EAP-TLS or PEAP with server validation for WLAN authentication.

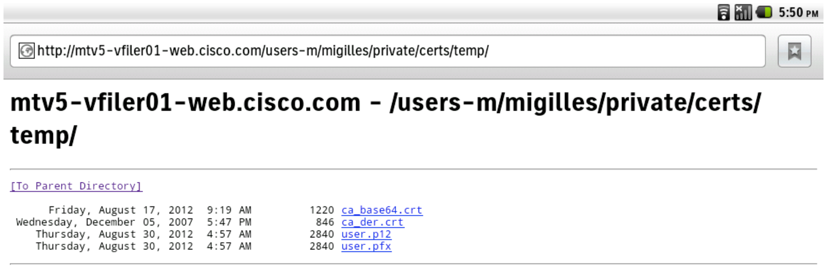
The user certificate must be in **PKCS #12** format (**.p12** extension), which contains the certificate and private key.

The CA certificate must be in **DER** or **Base-64** (**.crt** extension as the .cer format is not supported).

Once a certificate is installed, then it is deemed a secure device and a CA certificate is then required if utilizing PEAP. Certificates can be installed via a web browser download or via ADB push (**adb push *cert_name* /sdcard/*cert_name***)

Use the following guidelines for installing certificates on Cisco Cius.

- To install a certificate via the web browser, simply navigate to the certificate then select it.
- If a certificate is copied to Cisco Cius via ADB push, then select the **Install from SD card** option.

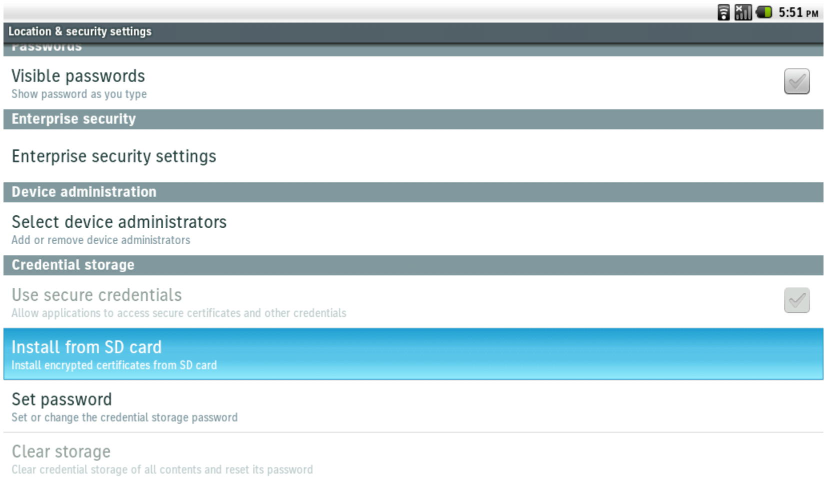


http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp/

mtv5-vfiler01-web.cisco.com - /users-m/migilles/private/certs/temp/

```
[To Parent Directory]

      Friday, August 17, 2012  9:19 AM        1220 ca_base64.crt
 Wednesday, December 05, 2007  5:47 PM         846 ca_der.crt
    Thursday, August 30, 2012  4:57 AM        2840 user.p12
    Thursday, August 30, 2012  4:57 AM        2840 user.pfx
```



Visible passwords ☑
Show password as you type

Enterprise security

Enterprise security settings

Device administration

Select device administrators
Add or remove device administrators

Credential storage

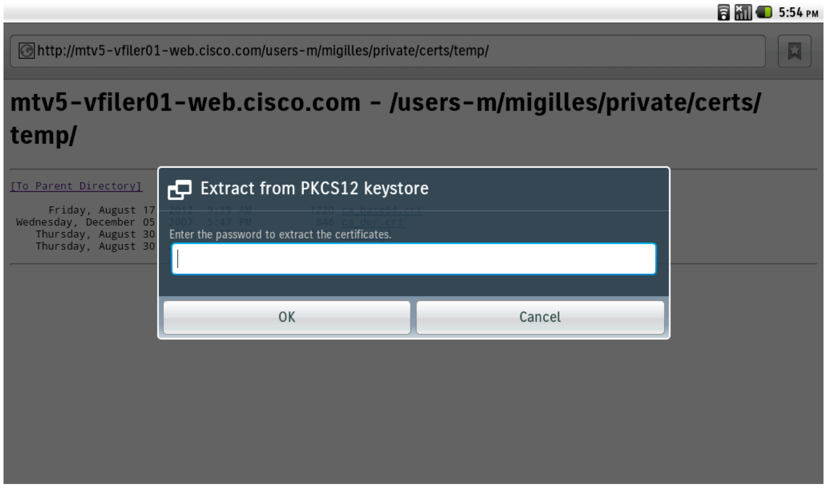
Use secure credentials ☑
Allow applications to access secure certificates and other credentials

Install from SD card
Install encrypted certificates from SD card

Set password
Set or change the credential storage password

Clear storage
Clear credential storage of all contents and reset its password

- For the user certificate install, the password will need to be entered to extract the certificates and keys from the imported PKCS #12 file.
- After the password is entered, a prompt will be displayed to name the certificate during.

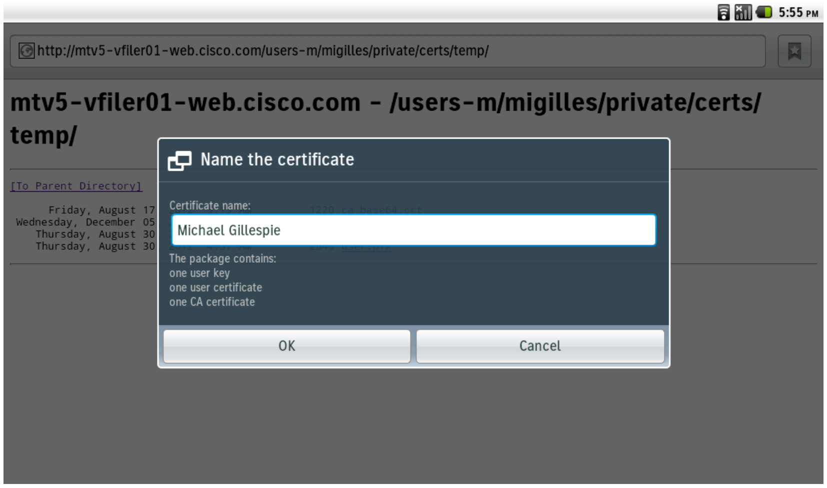


http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp/

mtv5-vfiler01-web.cisco.com - /users-m/migilles/private/certs/temp/

Extract from PKCS12 keystore

Enter the password to extract the certificates.



http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp/

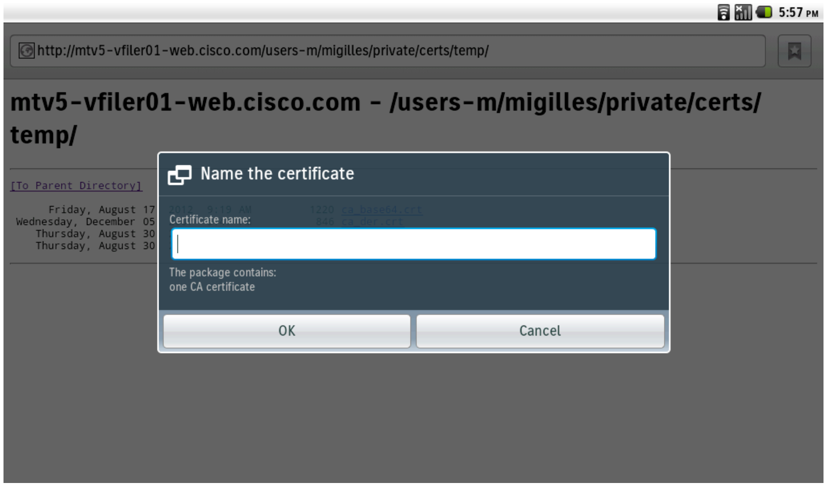
mtv5-vfiler01-web.cisco.com - /users-m/migilles/private/certs/temp/

Name the certificate

Certificate name: Michael Gillespie

The package contains:
one user key
one user certificate
one CA certificate

- For the CA certificate, simply name the certificate.



http://mtv5-vfiler01-web.cisco.com/users-m/migilles/private/certs/temp/

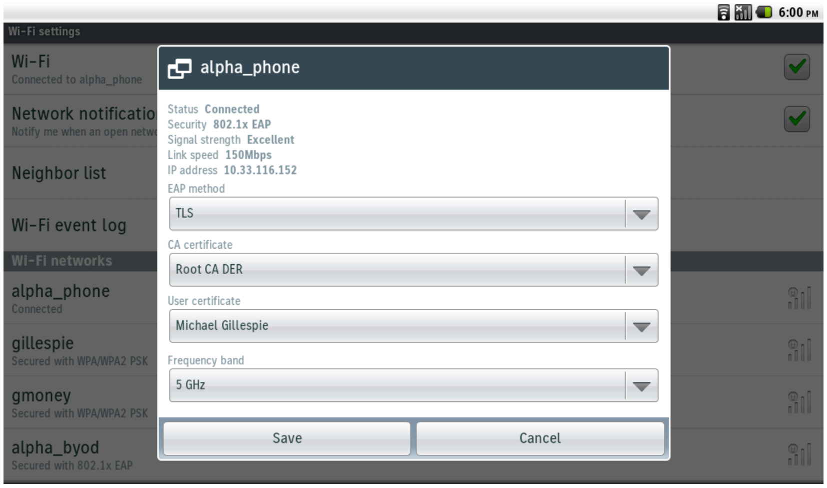
mtv5-vfiler01-web.cisco.com - /users-m/migilles/private/certs/temp/

Name the certificate

Certificate name:

The package contains:
one CA certificate

- Once the certificates are installed, they can then be utilized for EAP-TLS or PEAP with server validation.
- For EAP-TLS, the **User certificate** and **CA certificate** need to be configured.
- For PEAP with server validation, the **CA certificate** needs to be configured.



6:00 PM

Wi-Fi settings

Wi-Fi
Connected to alpha_phone

Network notificatio
Notify me when an open netw

Neighbor list

Wi-Fi event log

Wi-Fi networks

alpha_phone
Connected

gillespie
Secured with WPA/WPA2 PSK

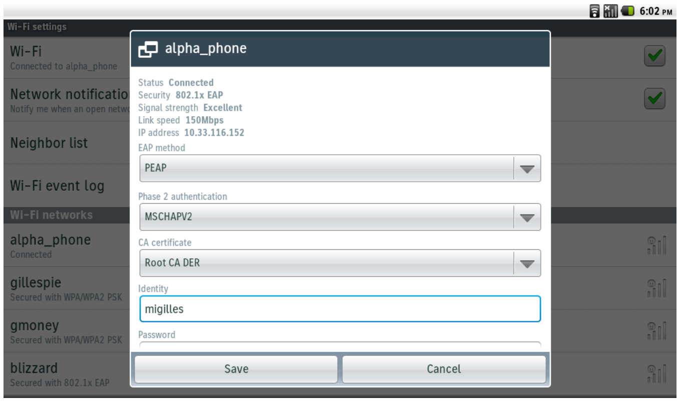
gmoney
Secured with WPA/WPA2 PSK

alpha_byod
Secured with 802.1x EAP

alpha_phone

Status Connected
Security 802.1x EAP
Signal strength Excellent
Link speed 150Mbps
IP address 10.33.116.152

EAP method: TLS
CA certificate: Root CA DER
User certificate: Michael Gillespie
Frequency band: 5 GHz



6:02 PM

Wi-Fi settings

Wi-Fi
Connected to alpha_phone

Network notificatio
Notify me when an open netw

Neighbor list

Wi-Fi event log

Wi-Fi networks

alpha_phone
Connected

gillespie
Secured with WPA/WPA2 PSK

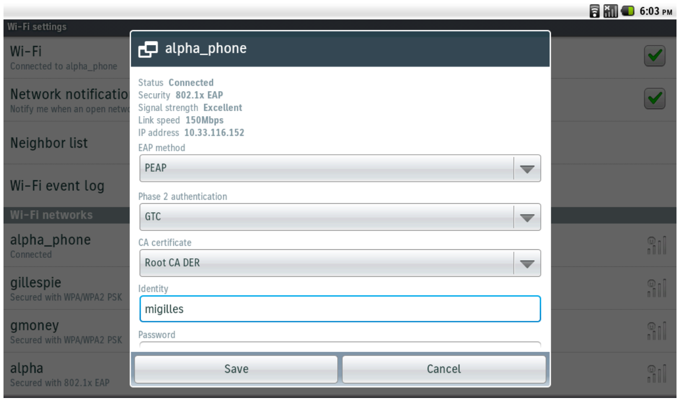
gmoney
Secured with WPA/WPA2 PSK

blizzard
Secured with 802.1x EAP

alpha_phone

Status Connected
Security 802.1x EAP
Signal strength Excellent
Link speed 150Mbps
IP address 10.33.116.152

EAP method: PEAP
Phase 2 authentication: MSCHAPV2
CA certificate: Root CA DER
Identity: migilles
Password



6:03 PM

Wi-Fi settings

Wi-Fi
Connected to alpha_phone

Network notificatio
Notify me when an open netw

Neighbor list

Wi-Fi event log

Wi-Fi networks

alpha_phone
Connected

gillespie
Secured with WPA/WPA2 PSK

gmoney
Secured with WPA/WPA2 PSK

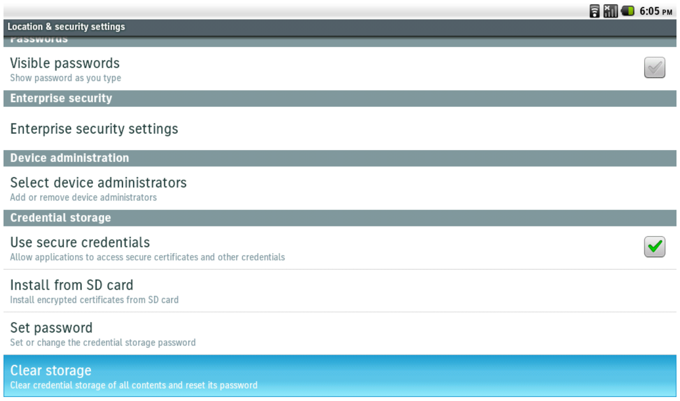
alpha
Secured with 802.1x EAP

alpha_phone

Status Connected
Security 802.1x EAP
Signal strength Excellent
Link speed 150Mbps
IP address 10.33.116.152

EAP method: PEAP
Phase 2 authentication: GTC
CA certificate: Root CA DER
Identity: migilles
Password

- To remove all certificates, select **Clear storage** in the Location & Security settings.



6:05 PM

Location & security settings

Passwords

Visible passwords
Show password as you type

Enterprise security

Enterprise security settings

Device administration

Select device administrators
Add or remove device administrators

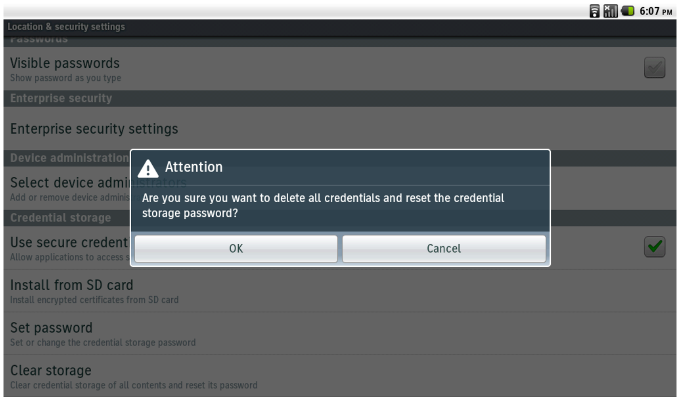
Credential storage

Use secure credentials ✓
Allow applications to access secure certificates and other credentials

Install from SD card
Install encrypted certificates from SD card

Set password
Set or change the credential storage password

Clear storage
Clear credential storage of all contents and reset its password



6:07 PM

Location & security settings

Attention

Are you sure you want to delete all credentials and reset the credential storage password?

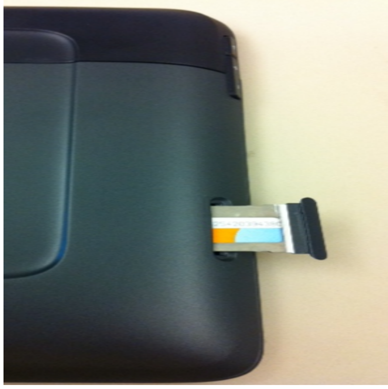
Mobile Network Settings

To utilize the mobile network functionality, first the SIM must be installed.

To install the SIM, slide out the SIM tray from the left side of Cisco Cius SP.

The face of the SIM should be facing towards the front of Cisco Cius SP (towards the display / face down if Cisco Cius is face down).

Once the SIM is aligned correctly in the tray, gently slide the SIM tray into the side of Cisco Cius SP where the SIM slot is located.



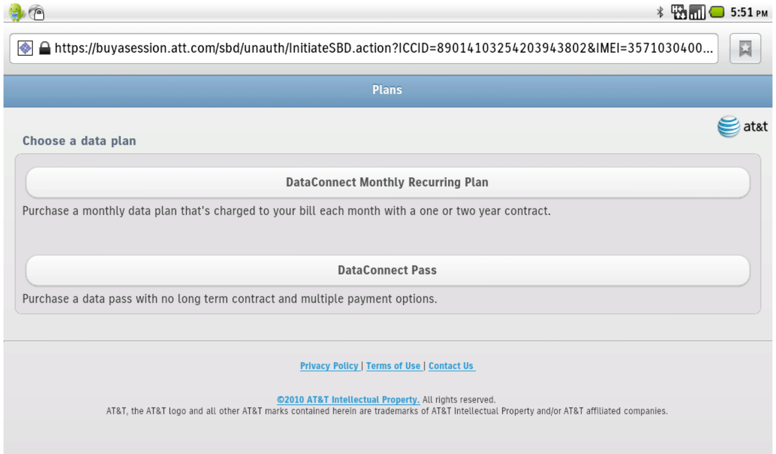
Currently only AT&T is offering data plans for Cisco Cius SP.

The following data plan options are available, which can be accessed by selecting **Add Data** on the AT&T Communication Manager widget.

- Sign a contract for a monthly recurring data plan.
- Purchase a data pass without a long-term contact.

If the **DataConnect Monthly Recurring Plan** option is selected, then the wizard to setup a contract for a monthly / recurring data plan will be displayed.

If the **DataConnect Pass** option is selected, then the wizard to obtain a pass without a long-term contact will be displayed.



https://buyasession.att.com/sbd/unauth/InitiateSBD.action?ICCID=89014103254203943802&IMEI=3571030400...

Plans

Choose a data plan

DataConnect Monthly Recurring Plan

Purchase a monthly data plan that's charged to your bill each month with a one or two year contract.

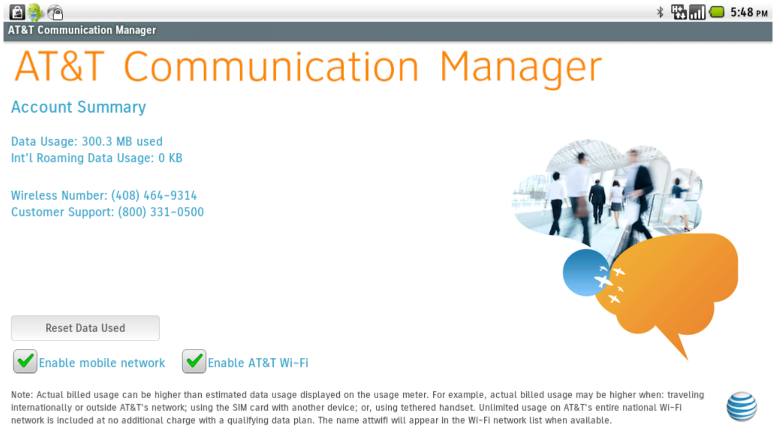
DataConnect Pass

Purchase a data pass with no long term contract and multiple payment options.

Privacy Policy | Terms of Use | Contact Us

©2010 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

The account summary can be displayed by launching the AT&T Communication Manager application or tapping on the AT&T Communication Manager widget on the display if configured.



AT&T Communication Manager

AT&T Communication Manager

Account Summary

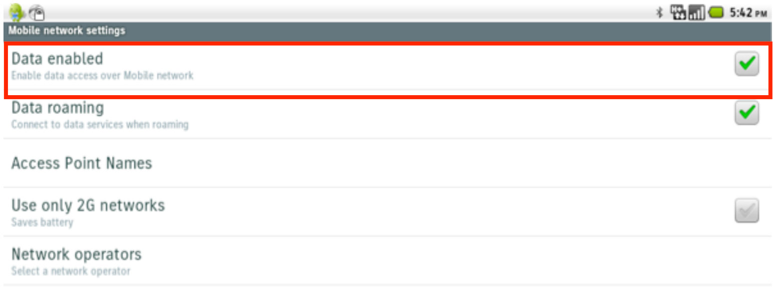
Data Usage: 300.3 MB used
Int'l Roaming Data Usage: 0 KB

Wireless Number: (408) 464-9314
Customer Support: (800) 331-0500

☑ Enable mobile network ☑ Enable AT&T Wi-Fi

Note: Actual billed usage can be higher than estimated data usage displayed on the usage meter. For example, actual billed usage may be higher when: traveling internationally or outside AT&T's network; using the SIM card with another device; or, using tethered handset. Unlimited usage on AT&T's entire national Wi-Fi network is included at no additional charge with a qualifying data plan. The name attwifi will appear in the Wi-Fi network list when available.

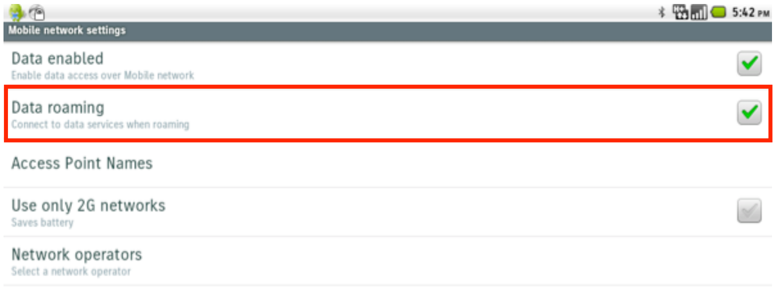
Data enabled in the mobile network settings must be selected in order to be able to connect to a mobile network.



Mobile network settings

- Data enabled — Enable data access over Mobile network ☑
- Data roaming — Connect to data services when roaming ☑
- Access Point Names
- Use only 2G networks — Saves battery ☐
- Network operators — Select a network operator

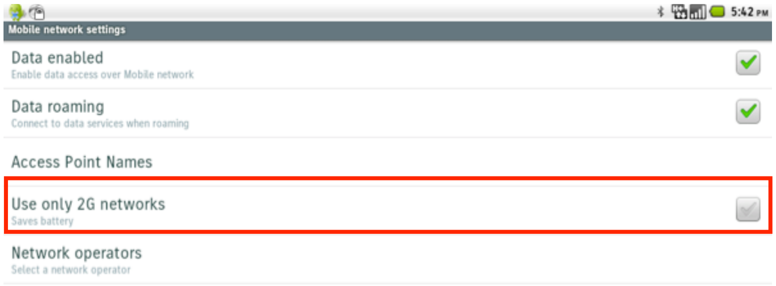
Data roaming in the mobile network settings must be selected in order to be able to connect to other service provider's mobile networks.



Mobile network settings

- Data enabled — Enable data access over Mobile network ☑
- Data roaming — Connect to data services when roaming ☑
- Access Point Names
- Use only 2G networks — Saves battery ☐
- Network operators — Select a network operator

If wanting to preserve battery life / reduce battery usage, **Use only 2G networks** can optionally be enabled, where Cisco Cius SP will connect to an EDGE (2G) mobile network.



Mobile network settings

- Data enabled — Enable data access over Mobile network ☑
- Data roaming — Connect to data services when roaming ☑
- Access Point Names
- Use only 2G networks — Saves battery ☐
- Network operators — Select a network operator

Bluetooth Settings

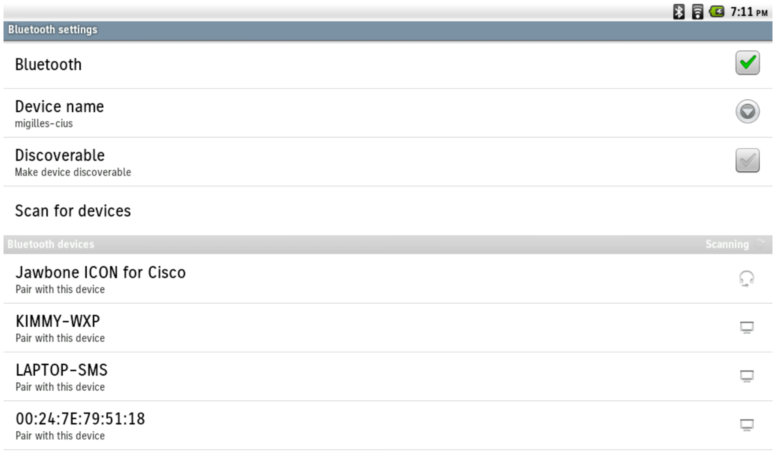
Cisco Cius has Bluetooth 2.1 + EDR (Enhanced Data Rate) support, which enables hands-free communications.

To pair a Bluetooth device to Cisco Cius, follow the instructions below.

- Navigate to **Settings** > **Wireless & networks** > **Bluetooth Settings**
- Ensure that **Bluetooth** is set to **On**.

  Ensure Bluetooth is enabled in the Cisco Unified Communications Manager; otherwise the option will be greyed out.
- Select **Scan for devices**.

  (Ensure the Bluetooth device is in pairing mode)
- Select the Bluetooth device after it is displayed in the list.
- Configure the Bluetooth device name for Cisco Cius as necessary by selecting **Device Name**.
- Cisco Cius visibility via Bluetooth can optionally be enabled temporarily by placing a check mark next to **Discoverable**.



7:11 PM

Bluetooth settings

Bluetooth ☑

Device name
migilles-cius

Discoverable ☐
Make device discoverable

Scan for devices

Bluetooth devices — Scanning

Jawbone ICON for Cisco
Pair with this device

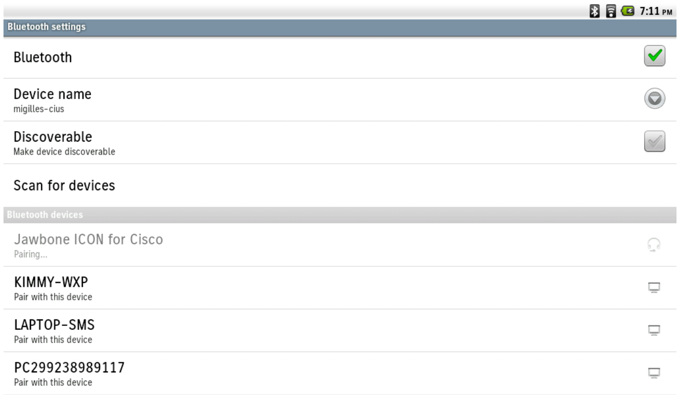
KIMMY-WXP
Pair with this device

LAPTOP-SMS
Pair with this device

00:24:7E:79:51:18
Pair with this device

- Cisco Cius will then attempt to pair will attempt to use the pin code **0000**.

  If unsuccessful, enter the pin code when prompted.
- Once paired, then Cisco Cius will attempt to connect to the Bluetooth device.



7:11 PM

Bluetooth settings

Bluetooth ☑

Device name
migilles-cius

Discoverable ☐
Make device discoverable

Scan for devices

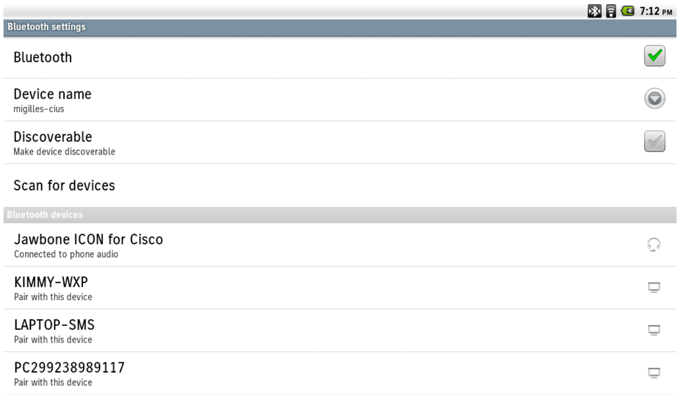
Bluetooth devices

Jawbone ICON for Cisco
Pairing...

KIMMY-WXP
Pair with this device

LAPTOP-SMS
Pair with this device

PC299238989117
Pair with this device



7:12 PM

Bluetooth settings

Bluetooth ☑

Device name
migilles-cius

Discoverable ☐
Make device discoverable

Scan for devices

Bluetooth devices

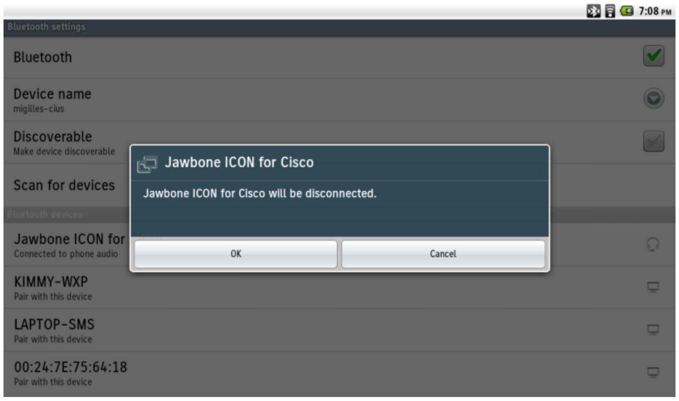
Jawbone ICON for Cisco
Connected to phone audio

KIMMY-WXP
Pair with this device

LAPTOP-SMS
Pair with this device

PC299238989117
Pair with this device

- Tapping the Bluetooth device then selecting **OK** will disconnect the currently connected Bluetooth device.



Bluetooth settings

Bluetooth ☑

Device name
migilles-cius

Discoverable
Make device discoverable

Scan for devices

Bluetooth devices

Jawbone ICON for
Connected to phone audio

KIMMY-WXP
Pair with this device

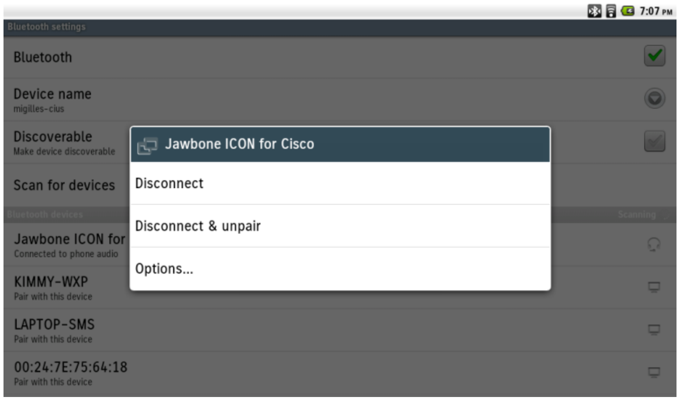
LAPTOP-SMS
Pair with this device

00:24:7E:75:64:18
Pair with this device

Jawbone ICON for Cisco

Jawbone ICON for Cisco will be disconnected.

- To unpair a Bluetooth device, select and hold the Bluetooth device selection then select **Disconnect & unpair**.
- Additional Bluetooth device options can be configured as well by selecting **Options**.



Bluetooth settings

Bluetooth ☑

Device name
migilles-cius

Discoverable
Make device discoverable

Scan for devices

Bluetooth devices

Jawbone ICON for
Connected to phone audio

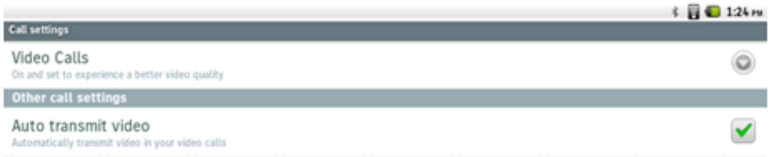
KIMMY-WXP
Pair with this device

LAPTOP-SMS
Pair with this device

00:24:7E:75:64:18
Pair with this device

Video Call Settings

Auto transmit video determines if Cisco Cius is to start streaming video immediately at the beginning of the call or not assuming the far end device has video capabilities. If disabled, the video can be unmuted at any time to start streaming video. This is enabled by default.



Call settings

Video Calls
On and set to experience a better video quality

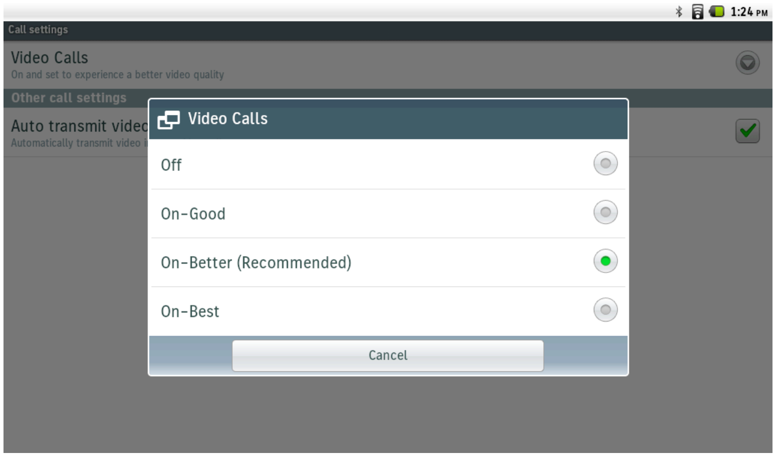
Other call settings

Auto transmit video ☑
Automatically transmit video in your video calls

The video call quality can be pre-defined in **Call Settings**.

Video can be disabled or enabled with 3 video quality options (Good, Better, Best).

- Good = CIF (352 x 288)
- Better = 360p (640 x 360)
- Best = 720p (1280 x 720)



1:24 PM

Call settings

Video Calls
On and set to experience a better video quality

Other call settings

Auto transmit video
Automatically transmit video

Video Calls

- Off ○
- On-Good ○
- On-Better (Recommended) ●
- On-Best ○

Cancel

Brightness can also be configured to accommodate for the current working environment.

Pressing the audio mute softkey will stop the transmitted audio.

Pressing the video mute softkey will stop the transmitted video.

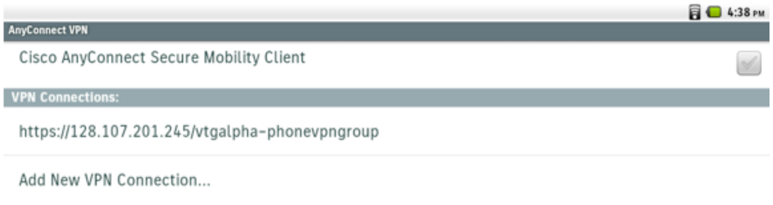
If the call is muted via the mute hard key, then the video is also muted.

When on a video call, the local video can be displayed along with the video of the remote endpoint.

VPN Settings

VPN connections can be configured if allowed by the administrator.

Enter the connection description and server address.



4:38 PM

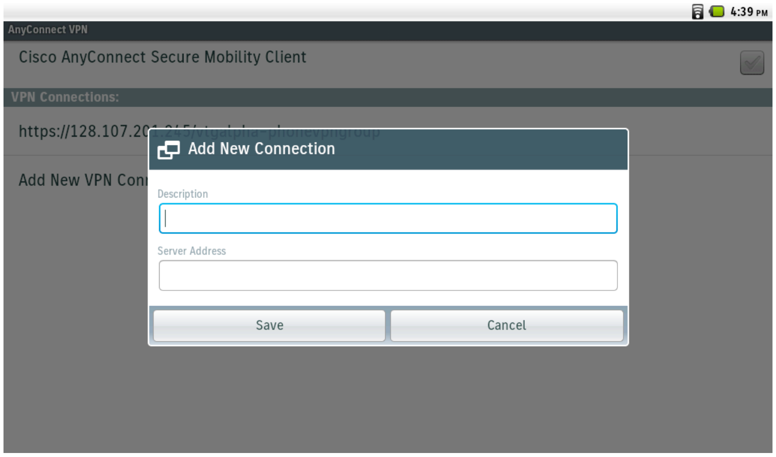
AnyConnect VPN

Cisco AnyConnect Secure Mobility Client ☑

VPN Connections:

https://128.107.201.245/vtgalpha-phonevpngroup

Add New VPN Connection...



4:39 PM

AnyConnect VPN

Cisco AnyConnect Secure Mobility Client ☑

VPN Connections:

Add New Connection

Description

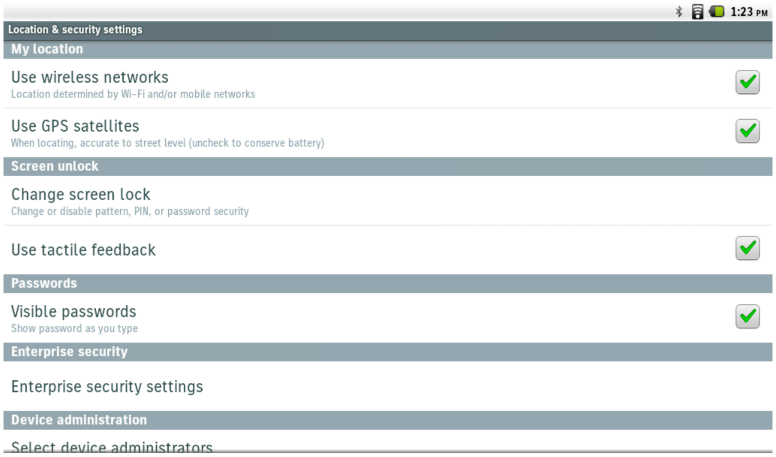
Server Address

Save Cancel

Location Settings

Location can be better determined via a current Wi-Fi connection, where that info can then be shared with applications.

Select **Use wireless networks**, in Location & security settings.



1:23 PM

Location & security settings

My location

Use wireless networks ☑
Location determined by Wi-Fi and/or mobile networks

Use GPS satellites ☑
When locating, accurate to street level (uncheck to conserve battery)

Screen unlock

Change screen lock
Change or disable pattern, PIN, or password security

Use tactile feedback ☑

Passwords

Visible passwords ☑
Show password as you type

Enterprise security

Enterprise security settings

Device administration

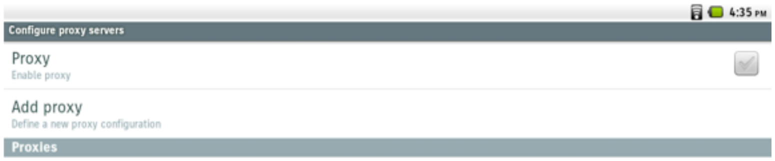
Select device administrators

Proxy Settings

Proxy settings can be configured by selecting **Proxy settings** in Wireless & network settings.

No proxy is configured by default.

Auto or Manual proxy mode can be optionally be enabled and configured.



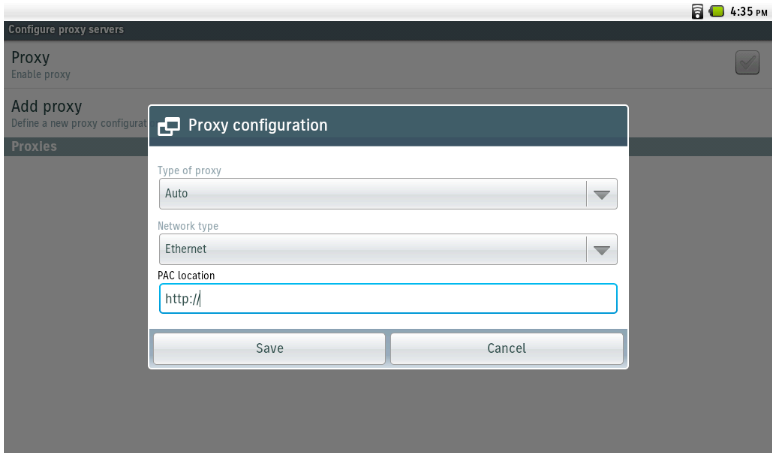
4:35 PM

Configure proxy servers

Proxy ☑
Enable proxy

Add proxy
Define a new proxy configuration

Proxies



4:35 PM

Configure proxy servers

Proxy ☑
Enable proxy

Add proxy
Define a new proxy configurat

Proxies

Proxy configuration

Type of proxy: Auto

Network type: Ethernet

PAC location: http://

Save | Cancel

Upgrading Firmware

To upgrade the firmware, install the signed COP file for Cisco Unified Communications Manager.

For information on how to install the COP file, refer to the Cisco Unified Communications Manager Operating System Administrator Guide at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

During TFTP server download, the configuration file is parsed and the device load is identified. Cisco Cius then downloads the firmware files to flash if it is not running the specified image already.

The Load Server can be specified as an alternate TFTP server to retrieve firmware files, which is located in the product specific configuration section of Cisco Cius within Cisco Unified Communications Manager Administration.

Using Cisco Cius

Application Markets

Various types of applications are available for download from Cisco AppHq or Google Play.

Cisco AppHq

Cisco AppHq is an application market that offers applications designed by Cisco, Cisco Solution Partners, and third-party Cius developers, which focuses on business-differentiated applications that integrate Cisco Unified Communications and Collaboration into the user experience.

Cisco AppHq offers applications such as Business, Communications, Education, Entertainment, Finance, Health and Fitness, Music and Audio, News, Photography, Productivity, Reference, Shopping, Social Networking, Sports, Tools and Utilities, Travel, Unified Communications, Video, Weather.

The **Cisco AppHq** application will be visible only if **Allow Applications from Cisco AppHQ** is enabled by the systems administrator in the Cisco Unified Communications Manager.

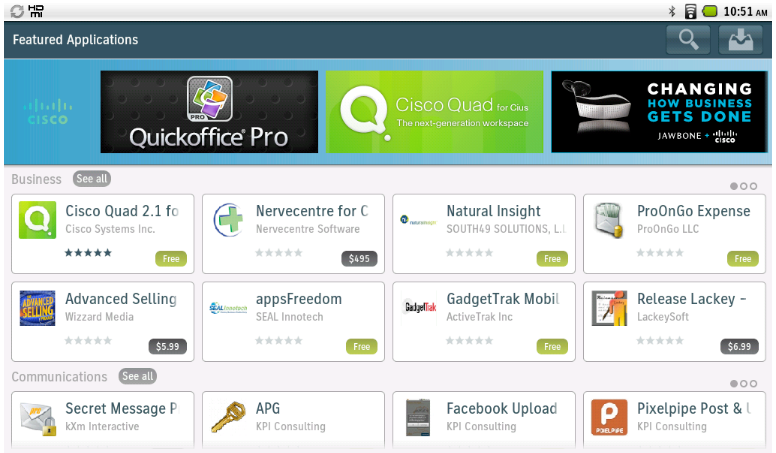
Allow Applications from Cisco AppHq

A Cisco AppHq account is necessary to download applications.

When first launching the Cisco AppHq, you will be prompted to sign in with your credentials or register if you do not have an account already.

The Cisco AppHq can also be accessed at this URL.

https://marketplace.cisco.com/apphq



Google Play

Google Play is an application market developed by Google™ for Android OS. The **Play Store** application allows users to browse and download applications published by third-party developers.

Google Play offers applications such as Books & Reference, Business, Comics, Communication, Education, Entertainment, Finance, Games, Health & Fitness, Libraries & Demo, Lifestyle, Live Wallpaper, Media & Video, Medical, Music & Audio, News & Magazines, Personalization, Photography, Productivity, Shopping, Social, Sports, Tools, Transportation, Travel & Local, Weather, and Widgets.

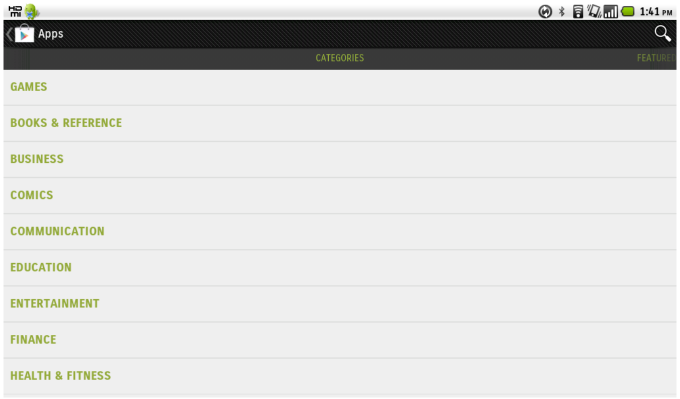
The **Play Store** application will be visible only if **Allow Applications from Android Market** is enabled by the systems administrator in the Cisco Unified Communications Manager.

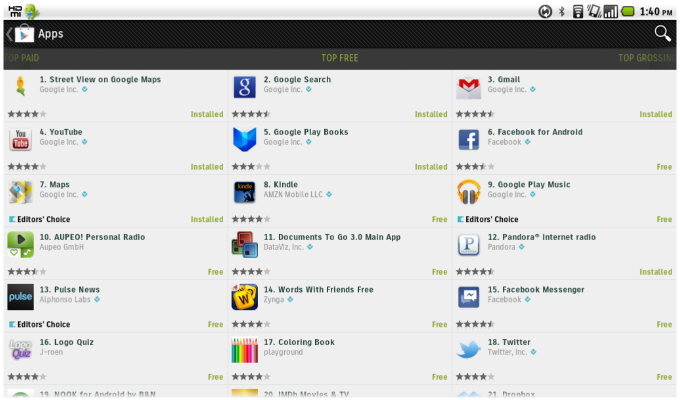
A Google account is necessary to download applications.

When first launching Google Play, you will be prompted to sign in with your credentials or register if you do not have an account already.

Google Play can also be accessed at this URL.

https://play.google.com/store



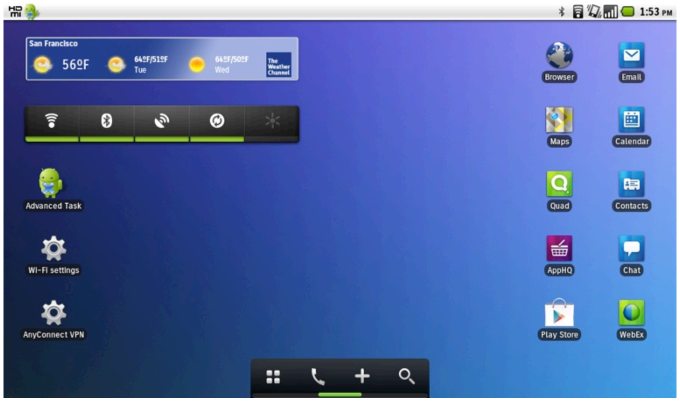


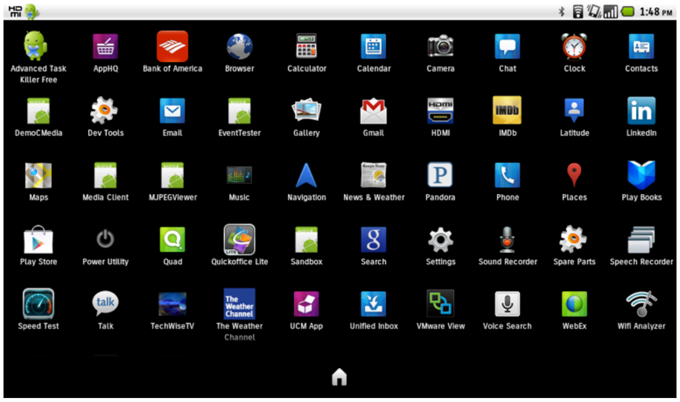
Applications

Aside of applications offered in Cisco AppHq and Google Play, there are pre-installed applications such as Cisco Unified Communications Manager Phone Client for voice and video calling, Cisco Unified Presence, Cisco Chat, Cisco WebEx, Cisco Quad, Email, Calendar and Contacts.

Phone Application

To launch the phone application, select the phone icon at the bottom of the main page, from the applications menu or from a shortcut created on the main page.

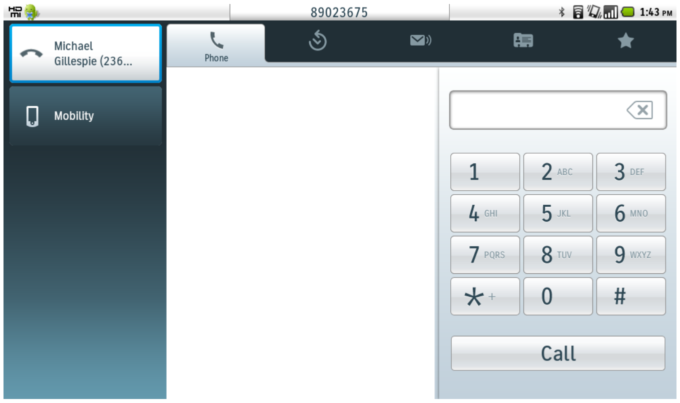


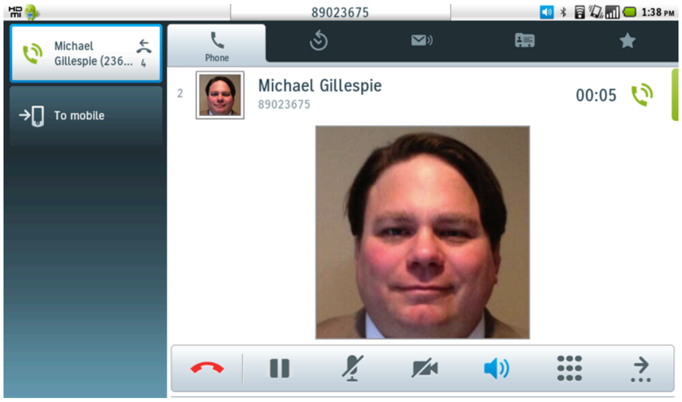


After the phone application is launched, the dial pad, call history, contacts and favorites menus are accessible.

Cisco Cius will attempt to register to Cisco Unified Communications Manager after power on, so the application does not have to be launched manually.

Cisco Cius is registered to Cisco Unified Communications Manager when the phone icon with name and/or extension are displayed.





Using the HD Media Station

The HD Media Station offers the following features.

- 10/100/1000 Gbps switch port for wired connection and Power over Ethernet (PoE); 2nd port for computer connection
- 3 USB ports
- 3.5 mm headset port
- Audio out port
- Additional speaker for wideband hands-free communications
- DisplayPort™ to connect to a larger display for an immersive video experience and for a virtualized desktop experience
- Two handset options (Standard and Slimline)

If powering Cisco Cius via inline power (PoE), the PoE switch will need to provide at least 24.9 watts in order to use the accessories (e.g. handset, speakerphone, etc.).

In order to have full functionality, Cisco Cius will need to be powered by a PoE+ (IEEE 802.3at standard) capable switch (e.g. Cisco Catalyst 3750-X Series Switches, Cisco Catalyst 3560-X Series Switches, etc.), which can provide up to 30 watts per port.

If utilizing a switch that is not PoE+ capable (e.g. Cisco Catalyst 3750 Series Switches or Cisco Catalyst 3750-E Series Switches), then only the Ethernet port will be activated and an AC power supply must be attached to the HD Media Station in order to use the additional accessories.

For more information on Cisco Switches, navigate to the following URL:

http://www.cisco.com/en/US/products/hw/switches/index.html

Cisco Cius will maintain voice, video and data communications without interruption when transitioning between docked and un-docked mode.

When WLAN and Ethernet interfaces are both in a connected state and Cisco Cius is in docked mode, then the call control (SIP) will traverse over the WLAN interface, where voice, video and data will traverse over the Ethernet interface for any new calls. The user then has the option to seamlessly transition to un-docked mode where the media (voice and video) will then traverse over the WLAN interface.

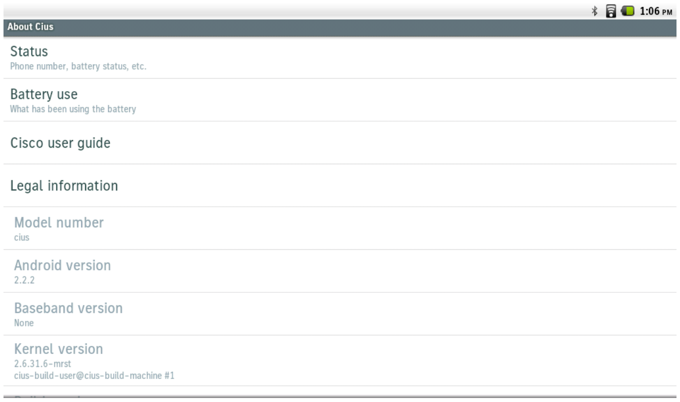
If Cisco Cius is currently un-docked and on a call via WLAN, the media (voice and video) for that current call will remain to traverse over the WLAN interface even if Cisco Cius is docked to an HD Media Station with an active Ethernet connection for the remainder of that call. Once that active call has ended, then the media for any future incoming or outgoing calls will traverse over the Ethernet connection, while the call control (SIP) will remain to traverse over the WLAN interface to allow for seamless undocking.

To decrease the time necessary to activate the Ethernet interface when docking Cisco Cius, the switch port that the HD media station is connected to can optionally be configured with **spanning-tree portfast**. Otherwise it will take 30 plus seconds before the Ethernet interface will be active.

Troubleshooting

About Cius

Status, battery usage and version information is displayed in **About Cius** in the Settings menu.



About Cius

Status
Phone number, battery status, etc.

Battery use
What has been using the battery

Cisco user guide

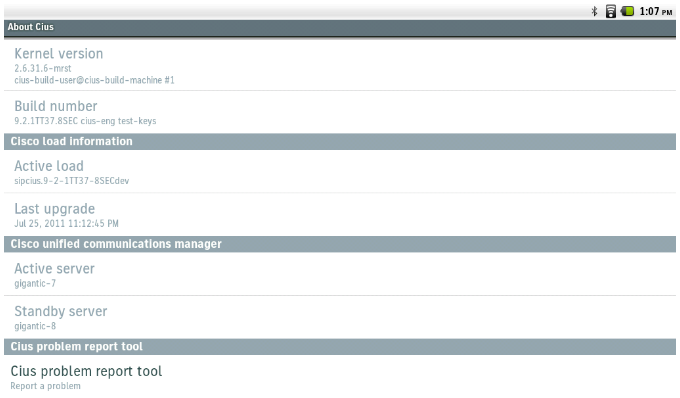
Legal information

Model number
cius

Android version
2.2.2

Baseband version
None

Kernel version
2.6.31.6-mrst
cius-build-user@cius-build-machine #1



About Cius

Kernel version
2.6.31.6-mrst
cius-build-user@cius-build-machine #1

Build number
9.2.1TT37.8SEC cius-eng test-keys

Cisco load information

Active load
sipcius.9-2-1TT37-8SECdev

Last upgrade
Jul 25, 2011 11:12:45 PM

Cisco unified communications manager

Active server
gigantic-7

Standby server
gigantic-8

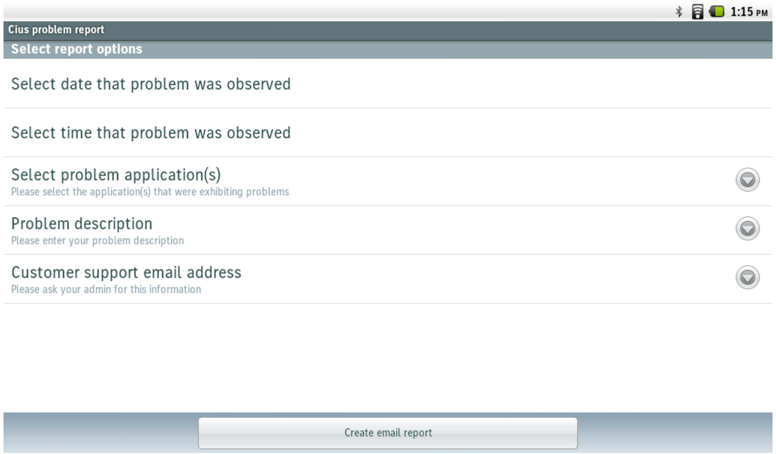
Cius problem report tool

Cius problem report tool
Report a problem

Cius Problem Report Tool

A problem report can be created via the Cius Problem Report Tool, which is located in the **About Cius** menu.

The date and time, problem application, problem description and customer support email address can be defined.



Cius problem report

Select report options

Select date that problem was observed

Select time that problem was observed

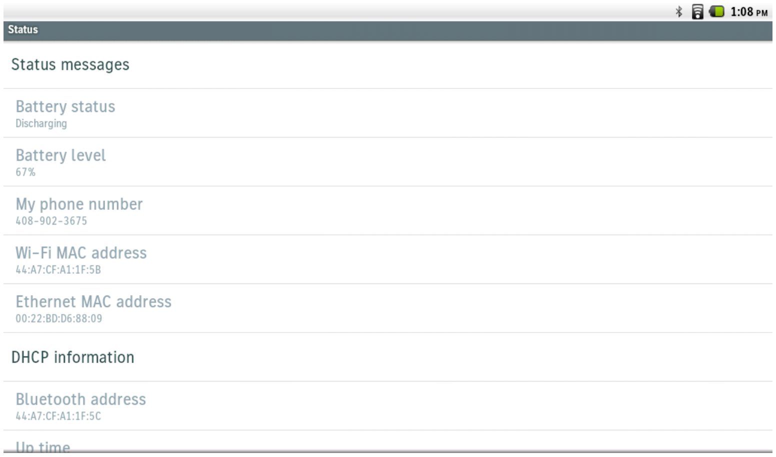
Select problem application(s)
Please select the application(s) that were exhibiting problems

Problem description
Please enter your problem description

Customer support email address
Please ask your admin for this information

Status

Status messages, battery status and level information, MAC address, DHCP information, up time, current access point and statistical information can be displayed by selecting **About Cius > Status**.



Status

Status messages

Battery status
Discharging

Battery level
67%

My phone number
408-902-3675

Wi-Fi MAC address
44:A7:CF:A1:1F:5B

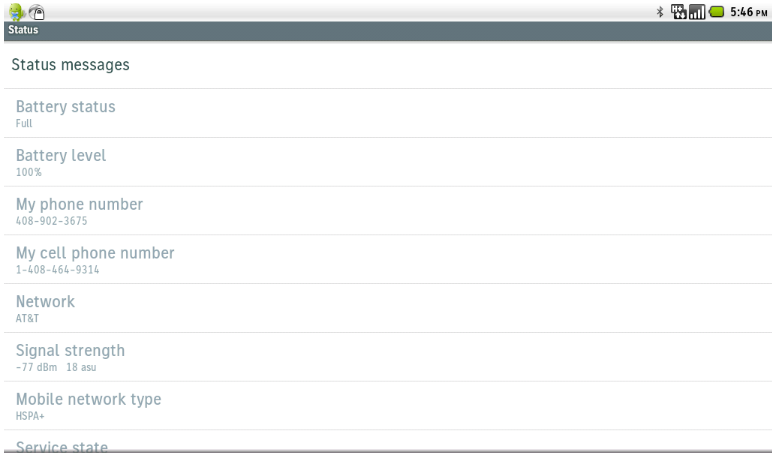
Ethernet MAC address
00:22:BD:D6:88:09

DHCP information

Bluetooth address
44:A7:CF:A1:1F:5C

Up time

When connected to HSPA+("4G"), the mobile network type will be displayed as such in the **About Cius > Status** menu.



Status

Status messages

Battery status
Full

Battery level
100%

My phone number
408-902-3675

My cell phone number
1-408-464-9314

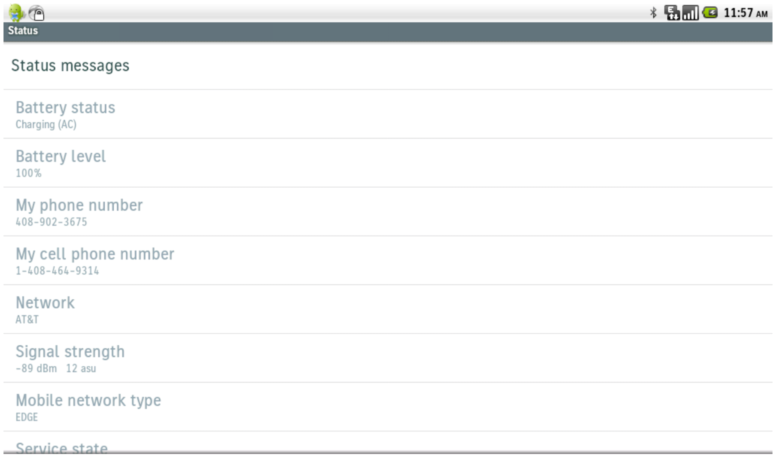
Network
AT&T

Signal strength
-77 dBm 18 asu

Mobile network type
HSPA+

Service state

When connected to EDGE (2G), the mobile network type will be displayed as such in the **About Cius > Status** menu.



11:57 AM

Status

Status messages

Battery status
Charging (AC)

Battery level
100%

My phone number
408-902-3675

My cell phone number
1-408-464-9314

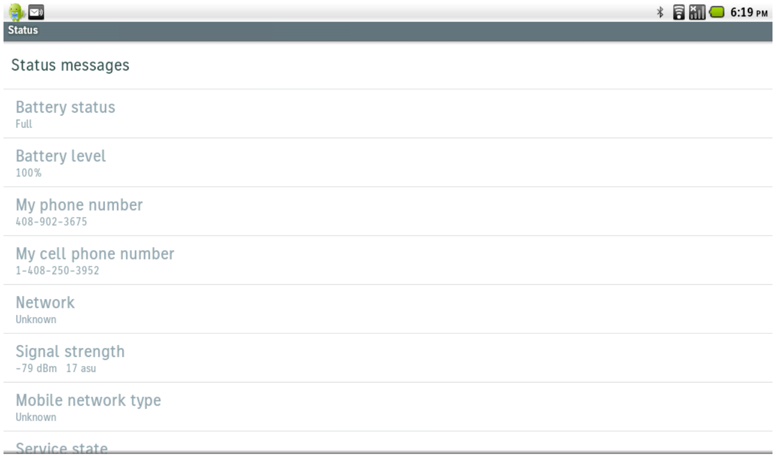
Network
AT&T

Signal strength
-89 dBm   12 asu

Mobile network type
EDGE

Service state

When not connected to a mobile network, there will not be any information for network, signal strength or mobile network type displayed in the **About Cius > Status** menu.



6:19 PM

Status

Status messages

Battery status
Full

Battery level
100%

My phone number
408-902-3675

My cell phone number
1-408-250-3952

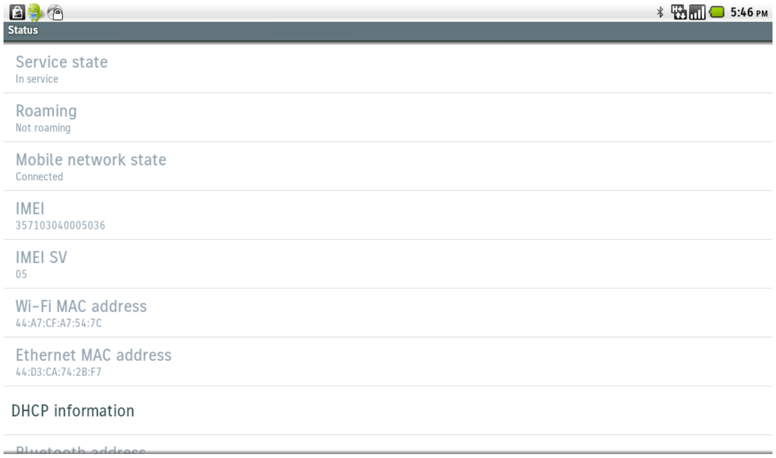
Network
Unknown

Signal strength
-79 dBm   17 asu

Mobile network type
Unknown

Service state

When connected to a mobile network, the **Service state** will be displayed as **In service** in the **About Cius > Status** menu; as well as displaying a connected signal indicator in the upper right of the display.



5:46 PM

Status

Service state
In service

Roaming
Not roaming

Mobile network state
Connected

IMEI
357103040005036

IMEI SV
05

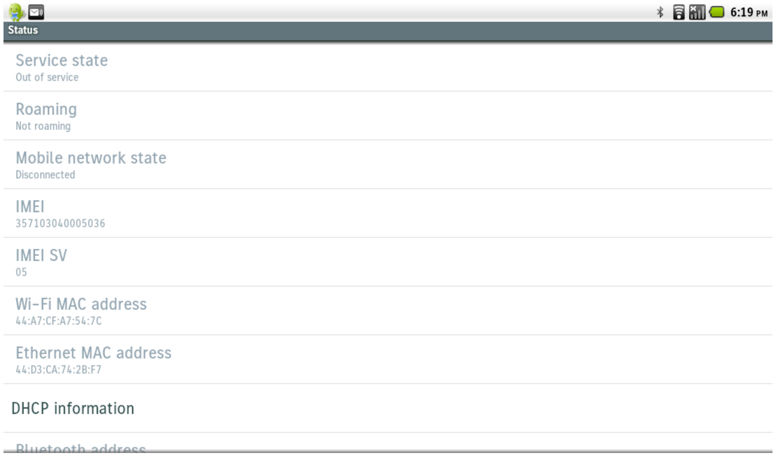
Wi-Fi MAC address
44:A7:CF:A7:54:7C

Ethernet MAC address
44:D3:CA:74:2B:F7

DHCP information

Bluetooth address

When not connected to a mobile network, the **Service state** will be displayed as **Out of service** in the **About Cius > Status** menu.



Status

Service state
Out of service

Roaming
Not roaming

Mobile network state
Disconnected

IMEI
357103040005036

IMEI SV
05

Wi-Fi MAC address
44:A7:CF:A7:54:7C

Ethernet MAC address
44:D3:CA:74:2B:F7

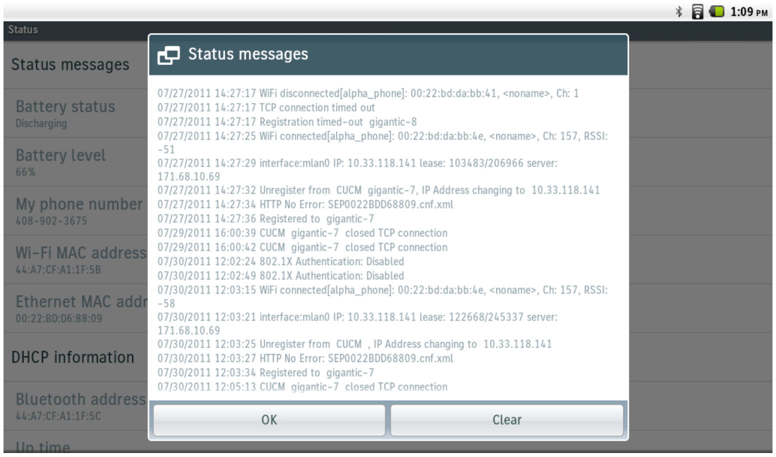
DHCP information

Bluetooth address

Status Messages

Select **Status messages** to display the message log.

Select **Clear** to reset the message log.



Status

Status messages

Battery status
Discharging

Battery level
66%

My phone number
408-902-3675

Wi-Fi MAC address
44:A7:CF:A1:1F:5B

Ethernet MAC addr
00:22:BD:D6:88:09

DHCP information

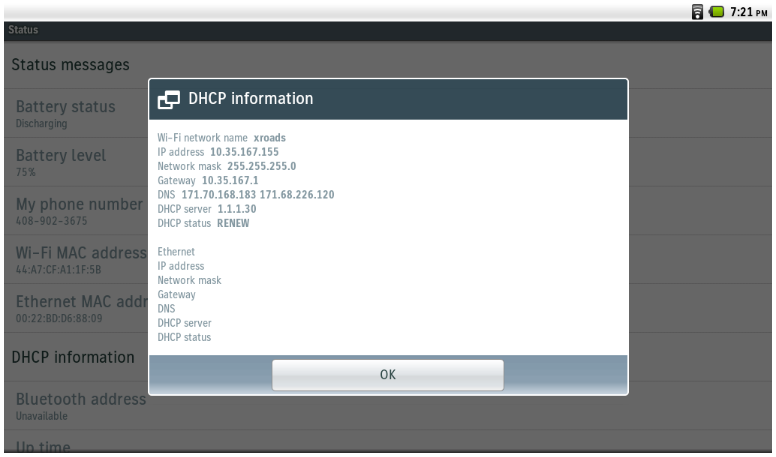
Bluetooth address
44:A7:CF:A1:1F:5C

Up time

Status messages

```
07/27/2011 14:27:17 WiFi disconnected[alpha_phone]: 00:22:bd:da:bb:41, <noname>, Ch: 1
07/27/2011 14:27:17 TCP connection timed out
07/27/2011 14:27:17 Registration timed-out  gigantic-8
07/27/2011 14:27:25 WiFi connected[alpha_phone]: 00:22:bd:da:bb:4e, <noname>, Ch: 157, RSSI:
-51
07/27/2011 14:27:29 interface:mlan0 IP: 10.33.118.141 lease: 103483/206966 server:
171.68.10.69
07/27/2011 14:27:32 Unregister from  CUCM  gigantic-7, IP Address changing to  10.33.118.141
07/27/2011 14:27:34 HTTP No Error: SEP0022BDD68809.cnf.xml
07/27/2011 14:27:36 Registered to  gigantic-7
07/29/2011 16:00:39 CUCM  gigantic-7  closed TCP connection
07/29/2011 16:00:42 CUCM  gigantic-7  closed TCP connection
07/30/2011 12:02:24 802.1X Authentication: Disabled
07/30/2011 12:02:49 802.1X Authentication: Disabled
07/30/2011 12:03:15 WiFi connected[alpha_phone]: 00:22:bd:da:bb:4e, <noname>, Ch: 157, RSSI:
-58
07/30/2011 12:03:21 interface:mlan0 IP: 10.33.118.141 lease: 122668/245337 server:
171.68.10.69
07/30/2011 12:03:25 Unregister from  CUCM  , IP Address changing to  10.33.118.141
07/30/2011 12:03:27 HTTP No Error: SEP0022BDD68809.cnf.xml
07/30/2011 12:03:34 Registered to  gigantic-7
07/30/2011 12:05:13 CUCM  gigantic-7  closed TCP connection
```

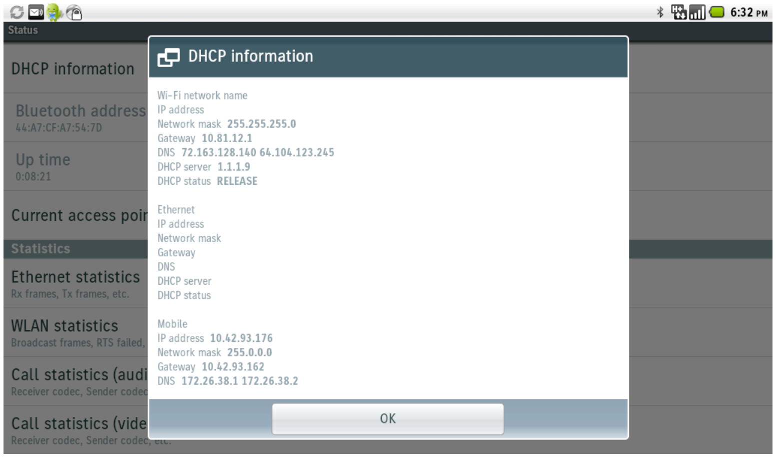
Select **DHCP information** to display the DHCP information for Wi-Fi, Ethernet, and Mobile interfaces.



DHCP information

Wi-Fi network name xroads
IP address 10.35.167.155
Network mask 255.255.255.0
Gateway 10.35.167.1
DNS 171.70.168.183 171.68.226.120
DHCP server 1.1.1.30
DHCP status RENEW

Ethernet
IP address
Network mask
Gateway
DNS
DHCP server
DHCP status



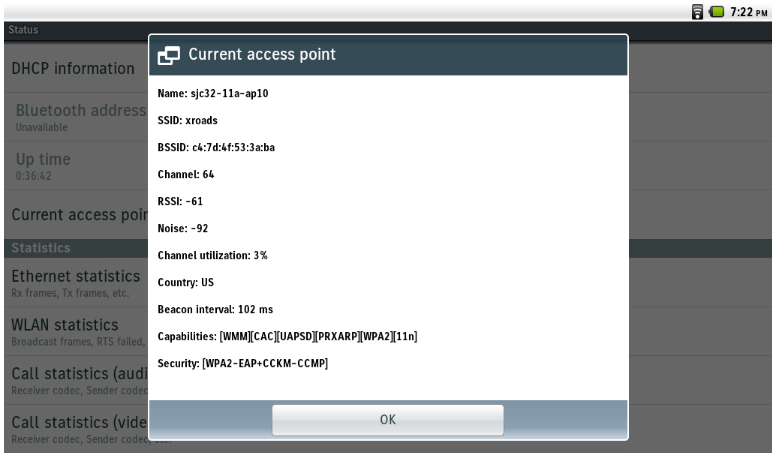
DHCP information

Wi-Fi network name
IP address
Network mask 255.255.255.0
Gateway 10.81.12.1
DNS 72.163.128.140 64.104.123.245
DHCP server 1.1.1.9
DHCP status RELEASE

Ethernet
IP address
Network mask
Gateway
DNS
DHCP server
DHCP status

Mobile
IP address 10.42.93.176
Network mask 255.0.0.0
Gateway 10.42.93.162
DNS 172.26.38.1 172.26.38.2

Select **Current access point** to display the details about the current access point connection.



Current access point

Name: sjc32-11a-ap10

SSID: xroads

BSSID: c4:7d:4f:53:3a:ba

Channel: 64

RSSI: -61

Noise: -92

Channel utilization: 3%

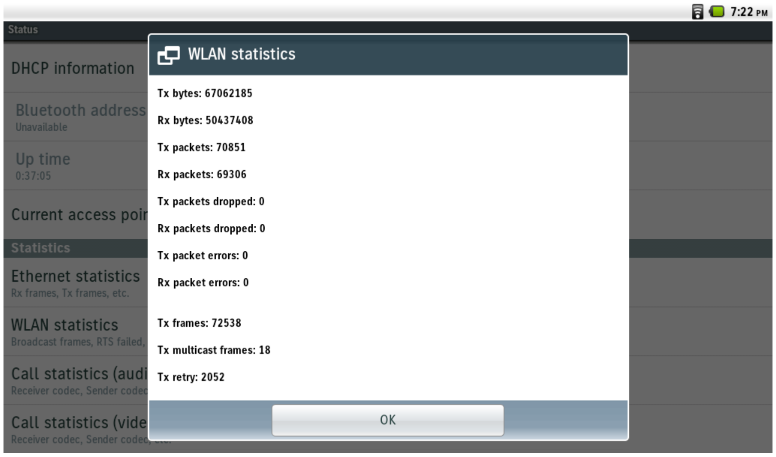
Country: US

Beacon interval: 102 ms

Capabilities: [WMM][CAC][UAPSD][PRXARP][WPA2][11n]

Security: [WPA2-EAP+CCKM-CCMP]

Select **WLAN statistics** to display transmitted and received byte, packet, packets dropped, packet error, and retry counter information.



WLAN statistics

Tx bytes: 67062185

Rx bytes: 50437408

Tx packets: 70851

Rx packets: 69306

Tx packets dropped: 0

Rx packets dropped: 0

Tx packet errors: 0

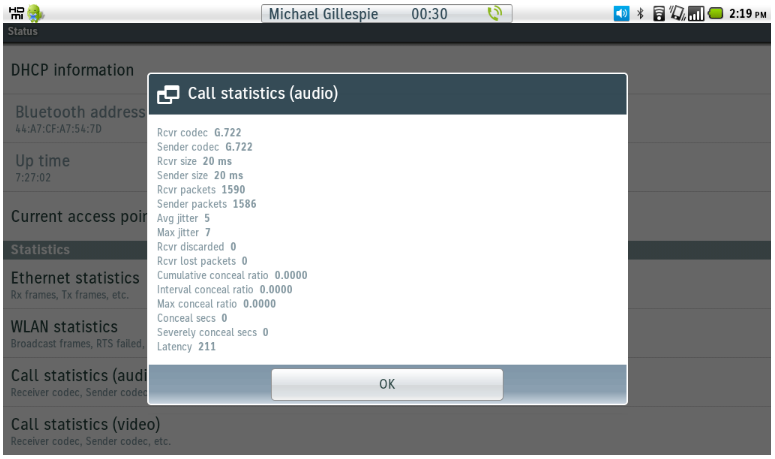
Rx packet errors: 0

Tx frames: 72538

Tx multicast frames: 18

Tx retry: 2052

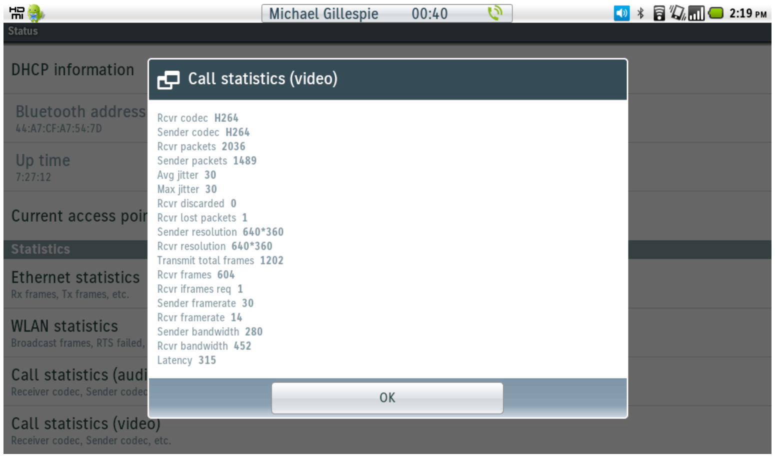
Select **Call statistics (audio)** to display the information about the current or last voice stream.



Call statistics (audio)

```
Rcvr codec  G.722
Sender codec  G.722
Rcvr size  20 ms
Sender size  20 ms
Rcvr packets  1590
Sender packets  1586
Avg jitter  5
Max jitter  7
Rcvr discarded  0
Rcvr lost packets  0
Cumulative conceal ratio  0.0000
Interval conceal ratio  0.0000
Max conceal ratio  0.0000
Conceal secs  0
Severely conceal secs  0
Latency  211
```

Select **Call statistics (video)** to display the information about the current or last video stream.



Call statistics (video)

```
Rcvr codec  H264
Sender codec  H264
Rcvr packets  2036
Sender packets  1489
Avg jitter  30
Max jitter  30
Rcvr discarded  0
Rcvr lost packets  1
Sender resolution  640*360
Rcvr resolution  640*360
Transmit total frames  1202
Rcvr frames  604
Rcvr iframes req  1
Sender framerate  30
Rcvr framerate  14
Sender bandwidth  280
Rcvr bandwidth  452
Latency  315
```

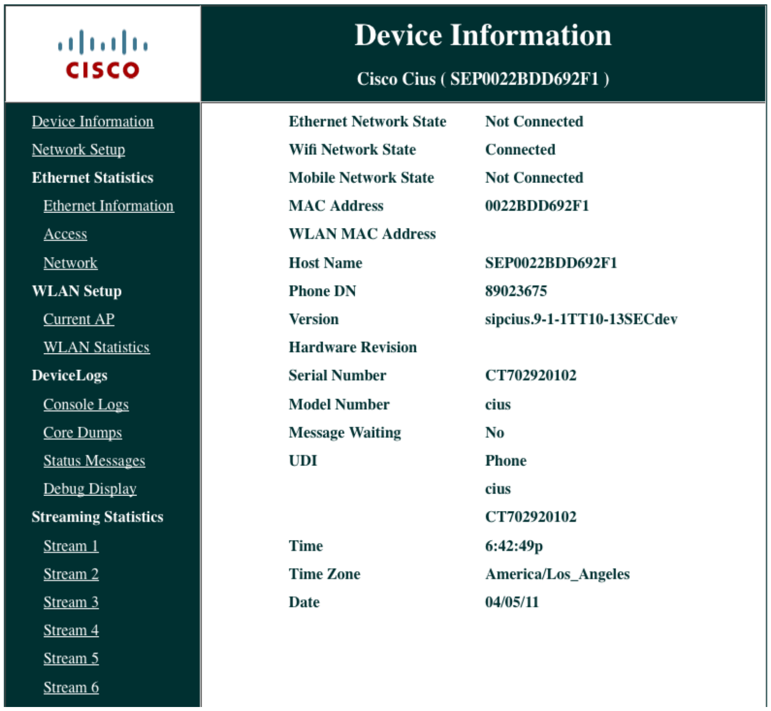
Device Webpage

The Cisco Cius webpage provides device information, network setup, WLAN setup, streaming and other statistical information as well as access to device logs.

Device Information

Cisco Cius provides device information, where network status, MAC address and version information is displayed.

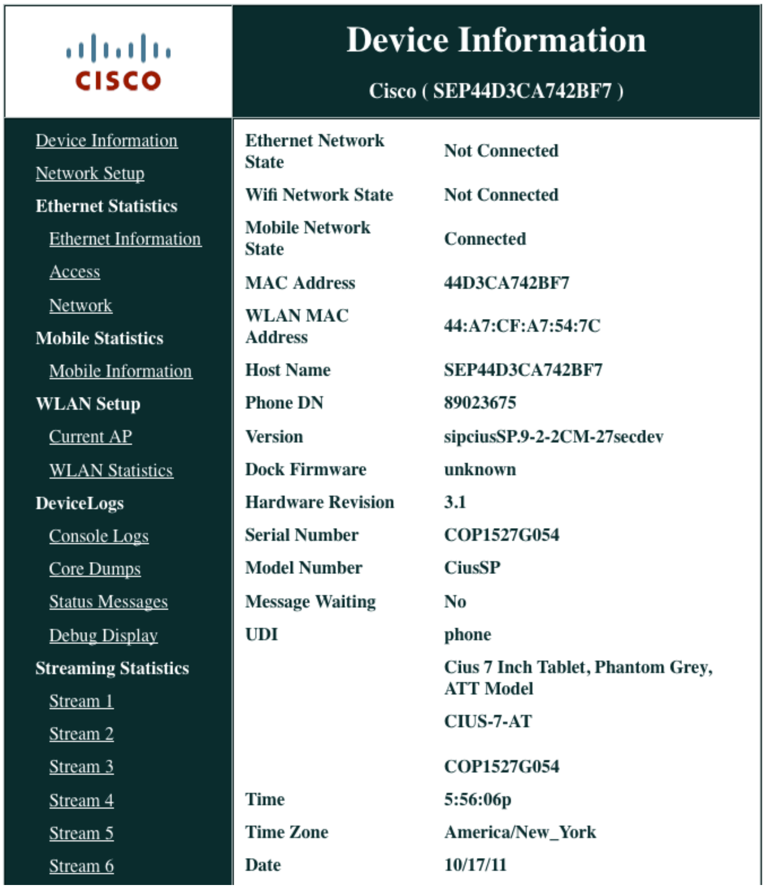
Browse to the web interface (http://x.x.x.x) of Cisco Cius then select **Device Information** to view this information.



Device Information

Cisco Cius (SEP0022BDD692F1)

Ethernet Network State	Not Connected
Wifi Network State	Connected
Mobile Network State	Not Connected
MAC Address	0022BDD692F1
WLAN MAC Address	
Host Name	SEP0022BDD692F1
Phone DN	89023675
Version	sipcius.9-1-1TT10-13SECdev
Hardware Revision	
Serial Number	CT702920102
Model Number	cius
Message Waiting	No
UDI	Phone
	cius
	CT702920102
Time	6:42:49p
Time Zone	America/Los_Angeles
Date	04/05/11



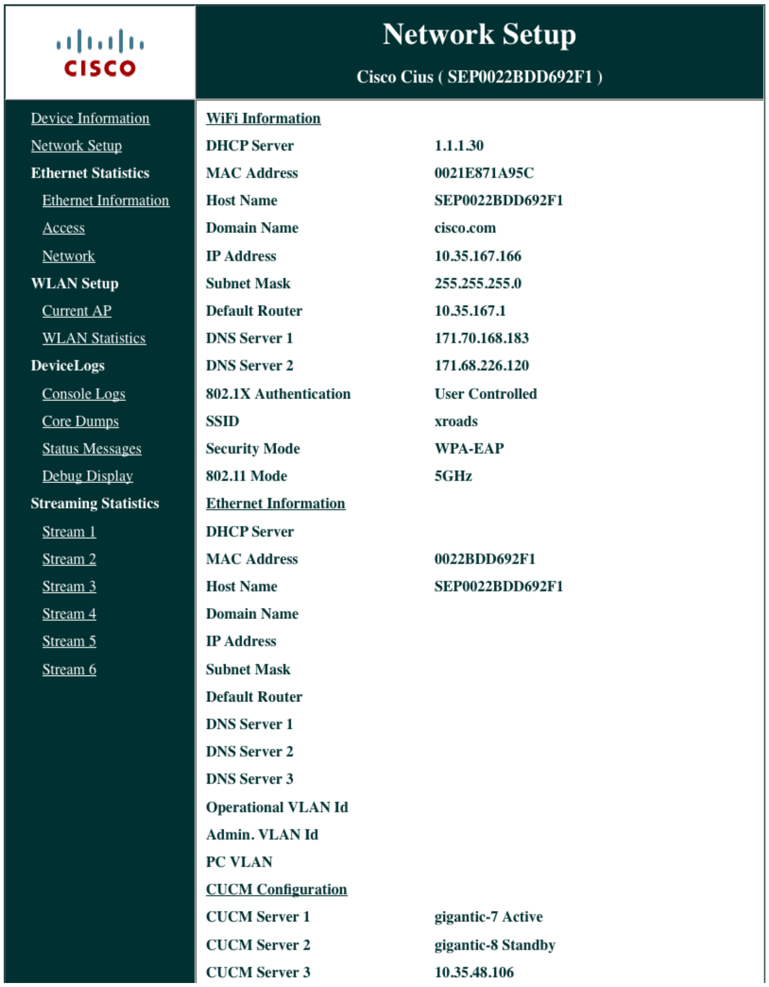
Cisco (SEP44D3CA742BF7)

Ethernet Network State	Not Connected
Wifi Network State	Not Connected
Mobile Network State	Connected
MAC Address	44D3CA742BF7
WLAN MAC Address	44:A7:CF:A7:54:7C
Host Name	SEP44D3CA742BF7
Phone DN	89023675
Version	sipciusSP.9-2-2CM-27secdev
Dock Firmware	unknown
Hardware Revision	3.1
Serial Number	COP1527G054
Model Number	CiusSP
Message Waiting	No
UDI	phone
	Cius 7 Inch Tablet, Phantom Grey, ATT Model
	CIUS-7-AT
	COP1527G054
Time	5:56:06p
Time Zone	America/New_York
Date	10/17/11

Network Setup

Cisco Cius provides network setup information, where Wi-Fi, Ethernet and Cisco Unified Communications Manager information is displayed.

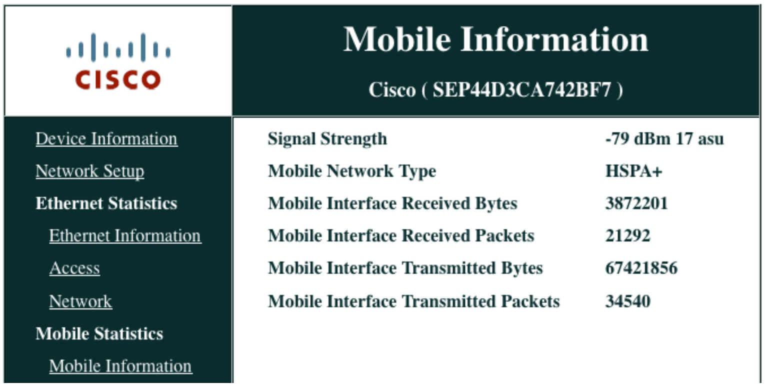
Browse to the web interface (http://x.x.x.x) of Cisco Cius then select **Network Setup** to view this information.



WiFi Information	
DHCP Server	1.1.1.30
MAC Address	0021E871A95C
Host Name	SEP0022BDD692F1
Domain Name	cisco.com
IP Address	10.35.167.166
Subnet Mask	255.255.255.0
Default Router	10.35.167.1
DNS Server 1	171.70.168.183
DNS Server 2	171.68.226.120
802.1X Authentication	User Controlled
SSID	xroads
Security Mode	WPA-EAP
802.11 Mode	5GHz
Ethernet Information	
DHCP Server	
MAC Address	0022BDD692F1
Host Name	SEP0022BDD692F1
Domain Name	
IP Address	
Subnet Mask	
Default Router	
DNS Server 1	
DNS Server 2	
DNS Server 3	
Operational VLAN Id	
Admin. VLAN Id	
PC VLAN	
CUCM Configuration	
CUCM Server 1	gigantic-7 Active
CUCM Server 2	gigantic-8 Standby
CUCM Server 3	10.35.48.106

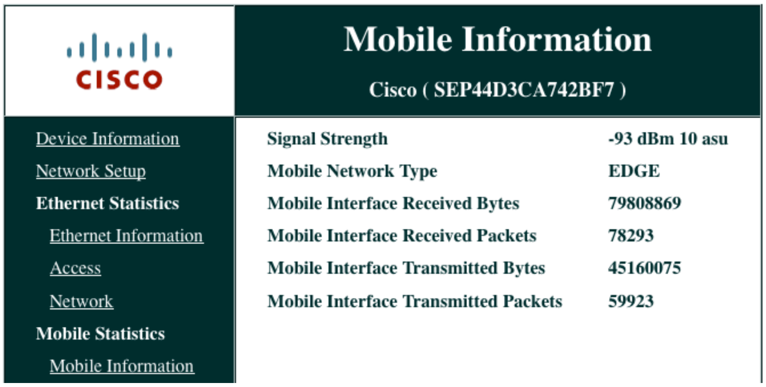
Mobile Information

When connected to HSPA+ (4G), the signal strength, mobile network type and packet counts will be displayed in the **Mobile Information** section of the Cisco Cius SP webpage.



Signal Strength	-79 dBm 17 asu
Mobile Network Type	HSPA+
Mobile Interface Received Bytes	3872201
Mobile Interface Received Packets	21292
Mobile Interface Transmitted Bytes	67421856
Mobile Interface Transmitted Packets	34540

When connected to EDGE (2G), the signal strength, mobile network type and packet counts will be displayed in the **Mobile Information** section of the Cisco Cius SP webpage.

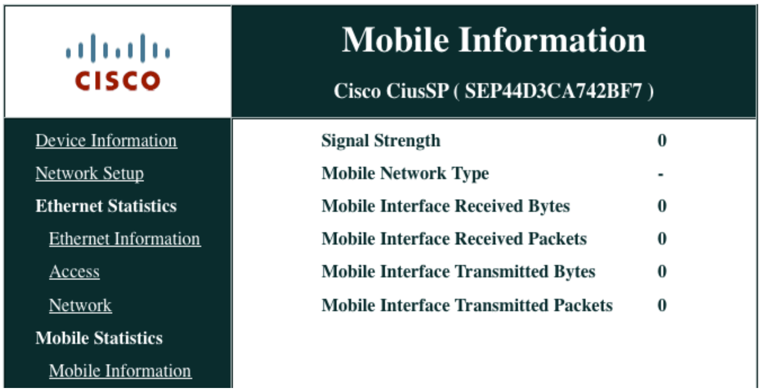


Mobile Information

Cisco (SEP44D3CA742BF7)

Signal Strength	-93 dBm 10 asu
Mobile Network Type	EDGE
Mobile Interface Received Bytes	79808869
Mobile Interface Received Packets	78293
Mobile Interface Transmitted Bytes	45160075
Mobile Interface Transmitted Packets	59923

When not connected to a mobile network, there will not be any information for signal strength, mobile network type and packet counts displayed in the **Mobile Information** section of the Cisco Cius SP webpage.



Mobile Information

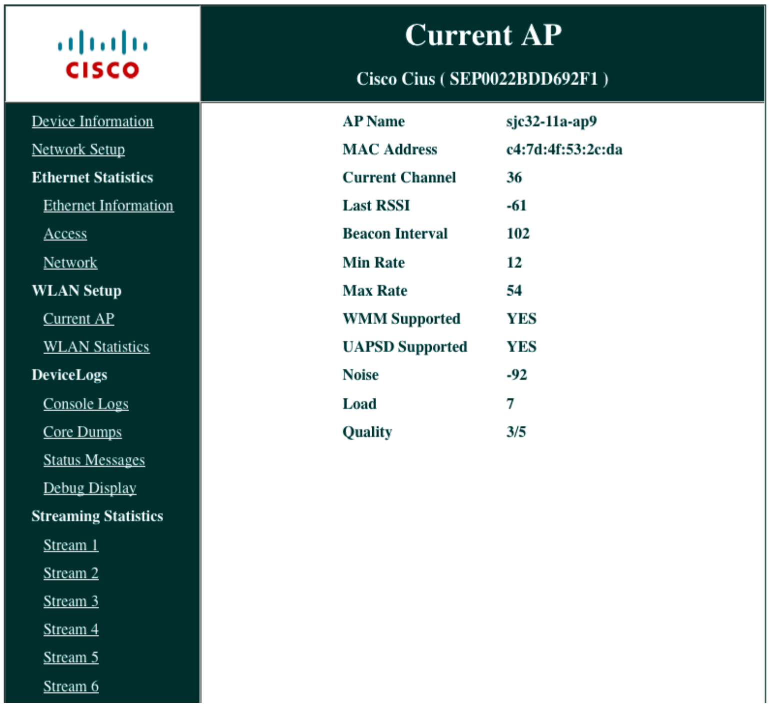
Cisco CiusSP (SEP44D3CA742BF7)

Signal Strength	0
Mobile Network Type	-
Mobile Interface Received Bytes	0
Mobile Interface Received Packets	0
Mobile Interface Transmitted Bytes	0
Mobile Interface Transmitted Packets	0

Current Access Point

Detailed information in regards to the current access point can also be seen in Cisco Cius' web interface.

Browse to the web interface (http://x.x.x.x) of Cisco Cius then select **Current AP** to view this information.



Current AP

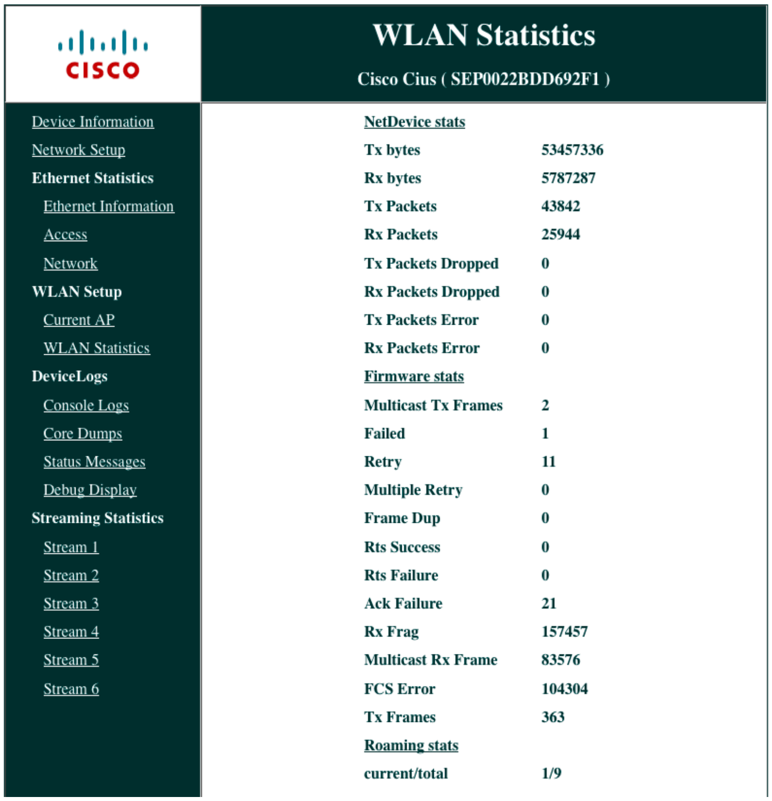
Cisco Cius (SEP0022BDD692F1)

AP Name	sjc32-11a-ap9
MAC Address	c4:7d:4f:53:2c:da
Current Channel	36
Last RSSI	-61
Beacon Interval	102
Min Rate	12
Max Rate	54
WMM Supported	YES
UAPSD Supported	YES
Noise	-92
Load	7
Quality	3/5

WLAN Statistics

Cisco Cius provides WLAN statistic information, where packet and counters are displayed.

Browse to the web interface (http://x.x.x.x) of Cisco Cius then select **WLAN Statistics** to view this information.



WLAN Statistics

Cisco Cius (SEP0022BDD692F1)

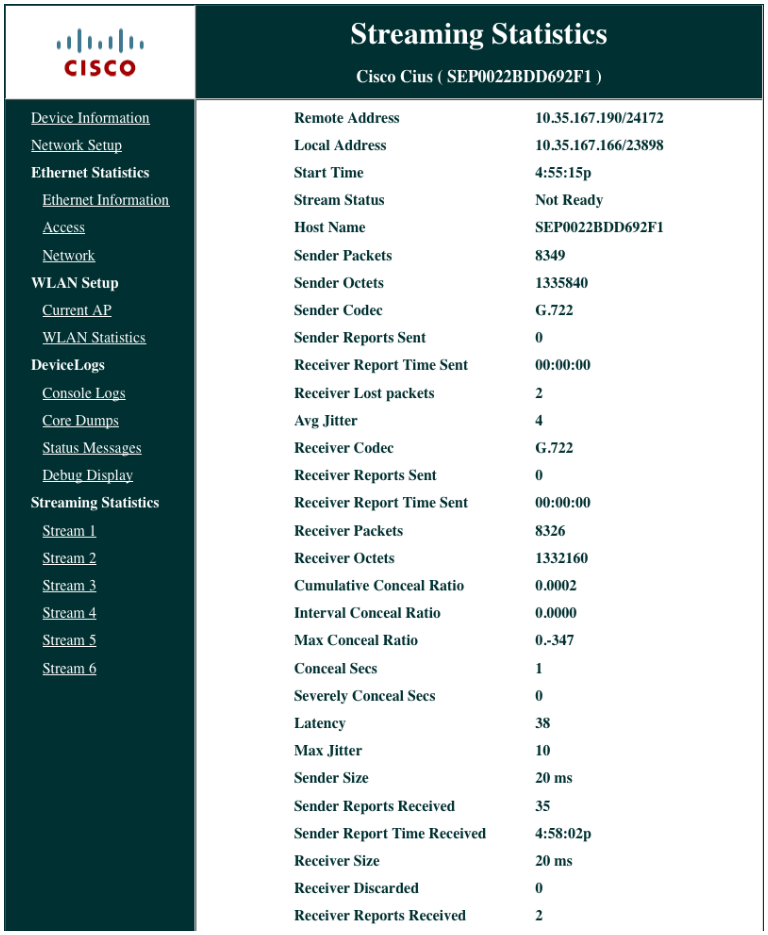
NetDevice stats	
Tx bytes	53457336
Rx bytes	5787287
Tx Packets	43842
Rx Packets	25944
Tx Packets Dropped	0
Rx Packets Dropped	0
Tx Packets Error	0
Rx Packets Error	0
Firmware stats	
Multicast Tx Frames	2
Failed	1
Retry	11
Multiple Retry	0
Frame Dup	0
Rts Success	0
Rts Failure	0
Ack Failure	21
Rx Frag	157457
Multicast Rx Frame	83576
FCS Error	104304
Tx Frames	363
Roaming stats	
current/total	1/9

Streaming Statistics

Cisco Cius provides call statistic information, where MOS, jitter and packet counters are displayed.

Browse to the web interface (http://x.x.x.x) of Cisco Cius then select **Streaming Statistics** to view this information.

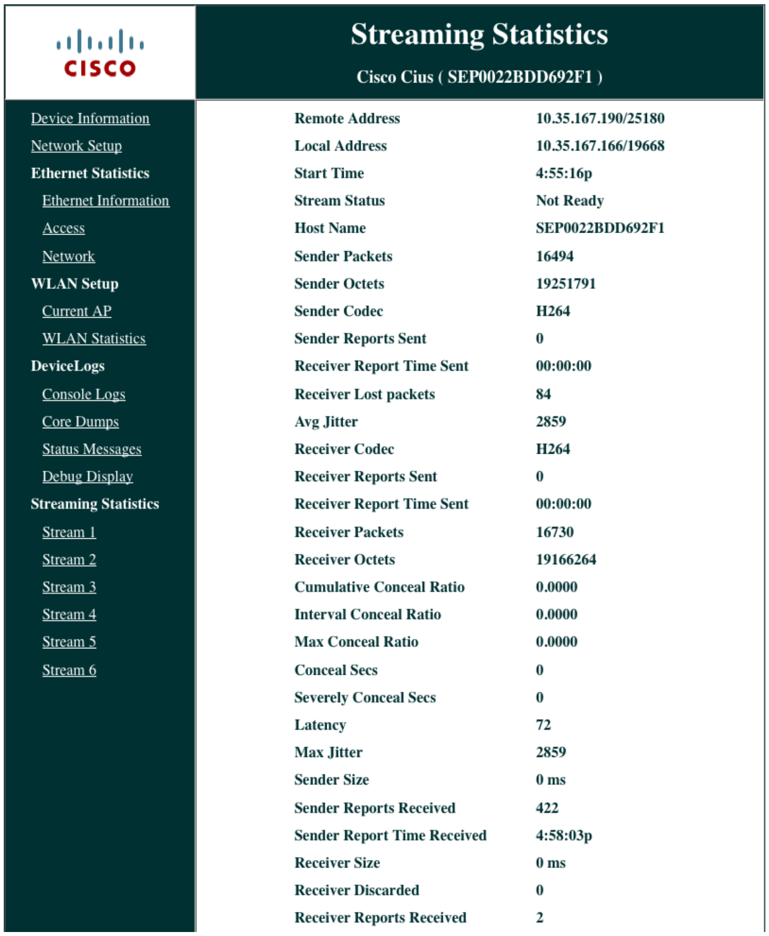
Cisco Cius does not display MOS (call quality) statistics for audio or video.



Streaming Statistics

Cisco Cius (SEP0022BDD692F1)

Remote Address	10.35.167.190/24172
Local Address	10.35.167.166/23898
Start Time	4:55:15p
Stream Status	Not Ready
Host Name	SEP0022BDD692F1
Sender Packets	8349
Sender Octets	1335840
Sender Codec	G.722
Sender Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Lost packets	2
Avg Jitter	4
Receiver Codec	G.722
Receiver Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Packets	8326
Receiver Octets	1332160
Cumulative Conceal Ratio	0.0002
Interval Conceal Ratio	0.0000
Max Conceal Ratio	0.-347
Conceal Secs	1
Severely Conceal Secs	0
Latency	38
Max Jitter	10
Sender Size	20 ms
Sender Reports Received	35
Sender Report Time Received	4:58:02p
Receiver Size	20 ms
Receiver Discarded	0
Receiver Reports Received	2



Streaming Statistics

Cisco Cius (SEP0022BDD692F1)

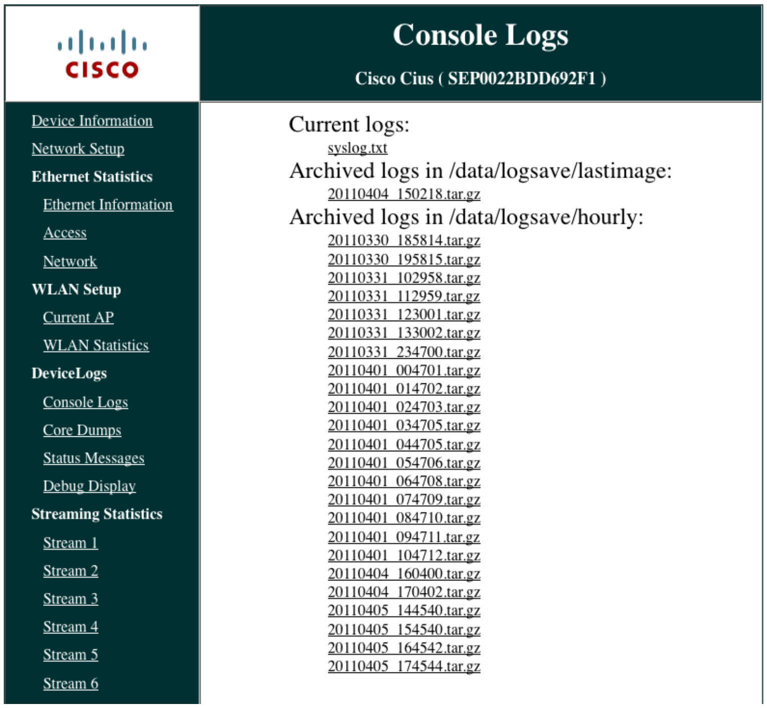
Remote Address	10.35.167.190/25180
Local Address	10.35.167.166/19668
Start Time	4:55:16p
Stream Status	Not Ready
Host Name	SEP0022BDD692F1
Sender Packets	16494
Sender Octets	19251791
Sender Codec	H264
Sender Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Lost packets	84
Avg Jitter	2859
Receiver Codec	H264
Receiver Reports Sent	0
Receiver Report Time Sent	00:00:00
Receiver Packets	16730
Receiver Octets	19166264
Cumulative Conceal Ratio	0.0000
Interval Conceal Ratio	0.0000
Max Conceal Ratio	0.0000
Conceal Secs	0
Severely Conceal Secs	0
Latency	72
Max Jitter	2859
Sender Size	0 ms
Sender Reports Received	422
Sender Report Time Received	4:58:03p
Receiver Size	0 ms
Receiver Discarded	0
Receiver Reports Received	2

For more information, see the **Troubleshooting Cisco Cius** chapter in the Cisco Cius Administration Guide at this URL: http://www.cisco.com/en/US/products/ps11156/prod_maintenance_guides_list.html

Device Logs

Console logs, core dumps, status messages for troubleshooting purposes can be obtained from the web interface of Cisco Cius.

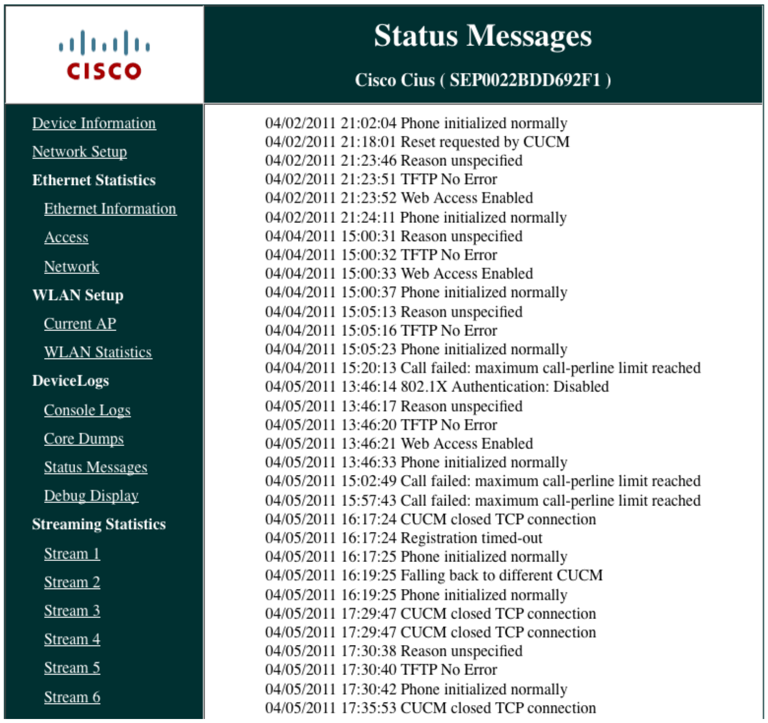
Browse to the web interface (http://x.x.x.x) of Cisco Cius then select the necessary menu item under **Device Logs** to view this information.



Console Logs

Cisco Cius (SEP0022BDD692F1)

Current logs:
syslog.txt
Archived logs in /data/logsave/lastimage:
20110404 150218.tar.gz
Archived logs in /data/logsave/hourly:
20110330 185814.tar.gz
20110330 195815.tar.gz
20110331 102958.tar.gz
20110331 112959.tar.gz
20110331 123001.tar.gz
20110331 133002.tar.gz
20110331 234700.tar.gz
20110401 004701.tar.gz
20110401 014702.tar.gz
20110401 024703.tar.gz
20110401 034705.tar.gz
20110401 044705.tar.gz
20110401 054706.tar.gz
20110401 064708.tar.gz
20110401 074709.tar.gz
20110401 084710.tar.gz
20110401 094711.tar.gz
20110401 104712.tar.gz
20110404 160400.tar.gz
20110404 170402.tar.gz
20110405 144540.tar.gz
20110405 154540.tar.gz
20110405 164542.tar.gz
20110405 174544.tar.gz



Status Messages

Cisco Cius (SEP0022BDD692F1)

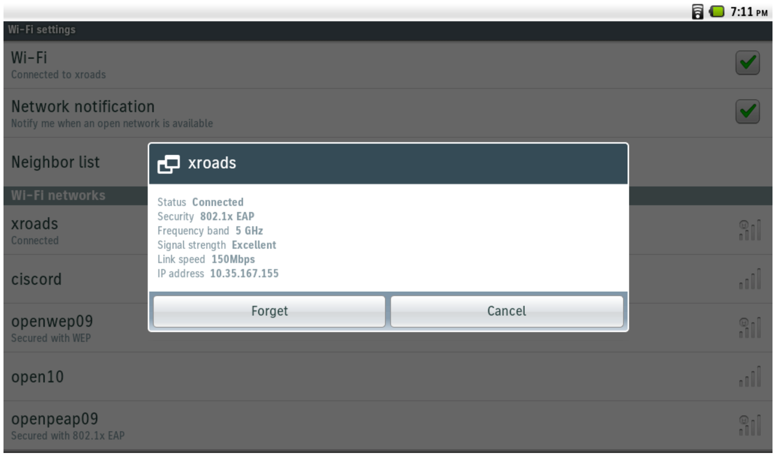
```
04/02/2011 21:02:04 Phone initialized normally
04/02/2011 21:18:01 Reset requested by CUCM
04/02/2011 21:23:46 Reason unspecified
04/02/2011 21:23:51 TFTP No Error
04/02/2011 21:23:52 Web Access Enabled
04/02/2011 21:24:11 Phone initialized normally
04/04/2011 15:00:31 Reason unspecified
04/04/2011 15:00:32 TFTP No Error
04/04/2011 15:00:33 Web Access Enabled
04/04/2011 15:00:37 Phone initialized normally
04/04/2011 15:05:13 Reason unspecified
04/04/2011 15:05:16 TFTP No Error
04/04/2011 15:05:23 Phone initialized normally
04/04/2011 15:20:13 Call failed: maximum call-perline limit reached
04/05/2011 13:46:14 802.1X Authentication: Disabled
04/05/2011 13:46:17 Reason unspecified
04/05/2011 13:46:20 TFTP No Error
04/05/2011 13:46:21 Web Access Enabled
04/05/2011 13:46:33 Phone initialized normally
04/05/2011 15:02:49 Call failed: maximum call-perline limit reached
04/05/2011 15:57:43 Call failed: maximum call-perline limit reached
04/05/2011 16:17:24 CUCM closed TCP connection
04/05/2011 16:17:24 Registration timed-out
04/05/2011 16:17:25 Phone initialized normally
04/05/2011 16:19:25 Falling back to different CUCM
04/05/2011 16:19:25 Phone initialized normally
04/05/2011 17:29:47 CUCM closed TCP connection
04/05/2011 17:29:47 CUCM closed TCP connection
04/05/2011 17:30:38 Reason unspecified
04/05/2011 17:30:40 TFTP No Error
04/05/2011 17:30:42 Phone initialized normally
04/05/2011 17:35:53 CUCM closed TCP connection
```

WLAN Information

Connection status, WLAN signal indicator, and neighbor list information can be displayed locally on Cisco Cius.

Connection Status

The current connection information including status, security type, frequency band, signal strength, link speed, and IP address can be displayed if the currently connected network is tapped.



7:11 PM

Wi-Fi settings

Wi-Fi ☑
Connected to xroads

Network notification ☑
Notify me when an open network is available

Neighbor list

Wi-Fi networks

xroads
Connected

ciscord

openwep09
Secured with WEP

open10

openpeap09
Secured with 802.1x EAP

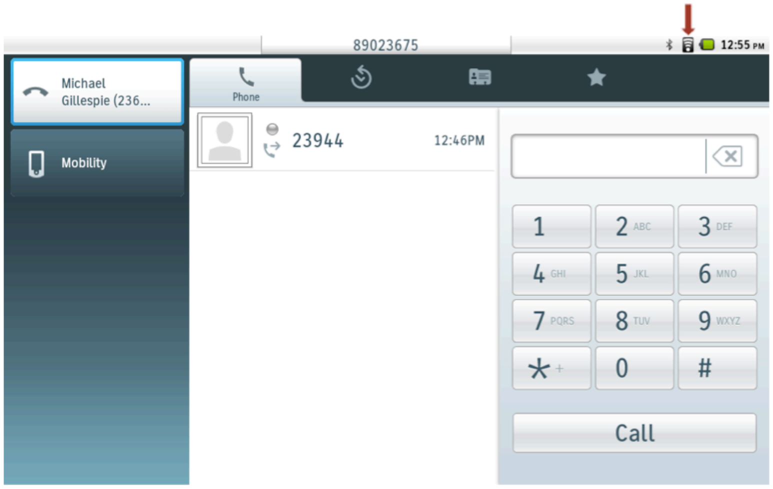
xroads

Status Connected
Security 802.1x EAP
Frequency band 5 GHz
Signal strength Excellent
Link speed 150Mbps
IP address 10.35.167.155

Forget | Cancel

WLAN Signal Indicator

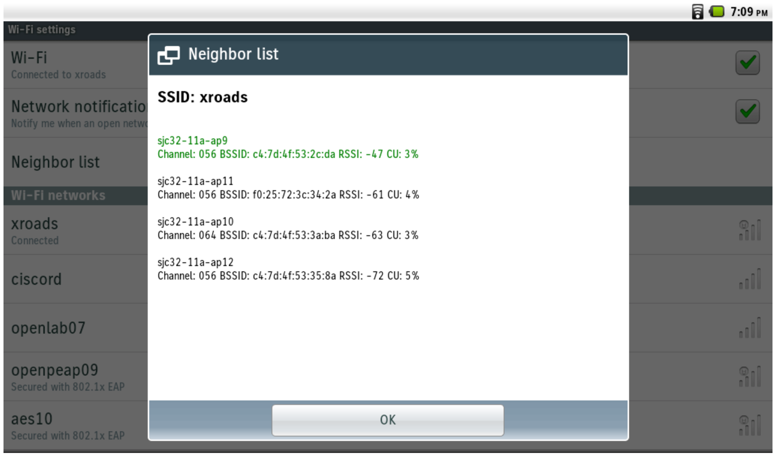
The WLAN signal indicator will always be visible in the upper right corner.



Neighbor List

Cisco Cius will display the current neighbors in the neighbor list menu.

To view the neighbor list, select **Neighbor list** within Wi-Fi Settings.



7:09 PM

Wi-Fi settings

Wi-Fi
Connected to xroads ☑

Network notificatio
Notify me when an open netw ☑

Neighbor list

Wi-Fi networks

xroads
Connected

ciscord

openlab07

openpeap09
Secured with 802.1x EAP

aes10
Secured with 802.1x EAP

Neighbor list

SSID: xroads

```
sjc32-11a-ap9
Channel: 056 BSSID: c4:7d:4f:53:2c:da RSSI: -47 CU: 3%

sjc32-11a-ap11
Channel: 056 BSSID: f0:25:72:3c:34:2a RSSI: -61 CU: 4%

sjc32-11a-ap10
Channel: 064 BSSID: c4:7d:4f:53:3a:ba RSSI: -63 CU: 3%

sjc32-11a-ap12
Channel: 056 BSSID: c4:7d:4f:53:35:8a RSSI: -72 CU: 5%
```

For more information, refer to the Cisco Cius Administration Guide at this URL:

http://www.cisco.com/en/US/products/ps11156/prod_maintenance_guides_list.html

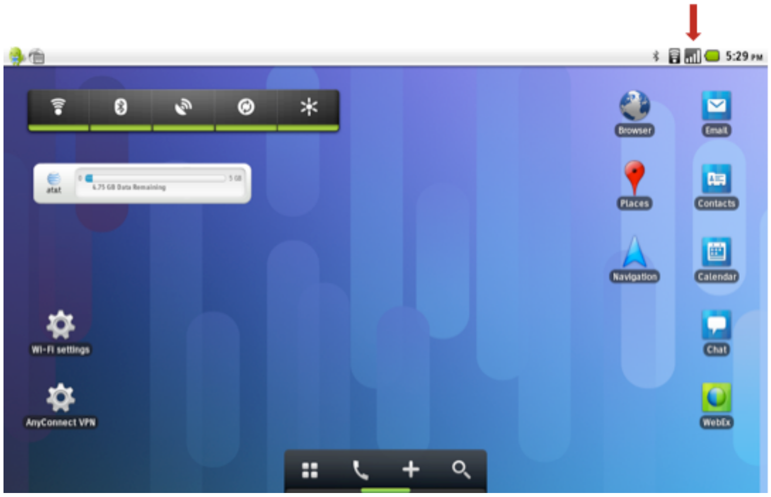
Mobile Network Information

Connection status, WLAN signal indicator, and neighbor list information can be displayed locally on Cisco Cius.

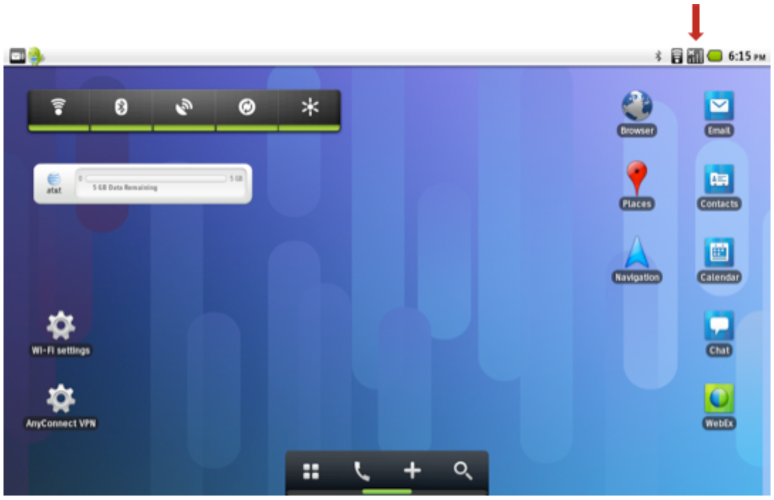
Mobile Network Signal Indicator

The Wireless LAN signal indicator in the top right will display, which will indicate current mobile network status.

If the mobile network is active / enabled, then a number of bars will be displayed assuming Cisco Cius SP is in good mobile network coverage and the SIM has been activated.

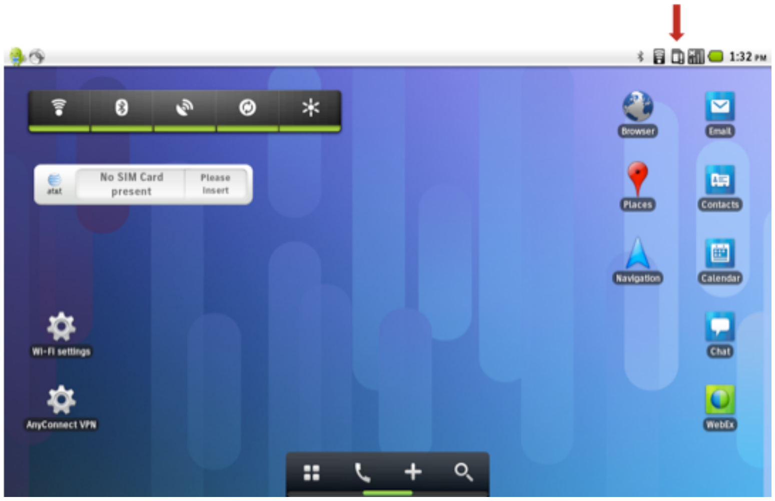


If the mobile network is inactive / disabled, then there will be not be any bars displayed plus an X in the upper left corner of the signal indicator, which indicates Cisco Cius SP is not in good mobile network coverage, the SIM has not been activated or the mobile network has been disabled locally on Cisco Cius SP.

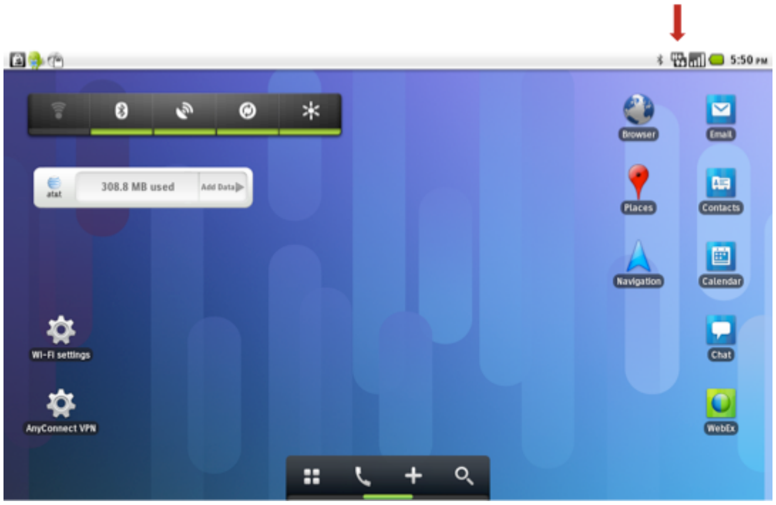


If Cisco Cius SP does not have a SIM inserted or can not detect the SIM, then there will be an icon with a SIM plus an exclamation point displayed.

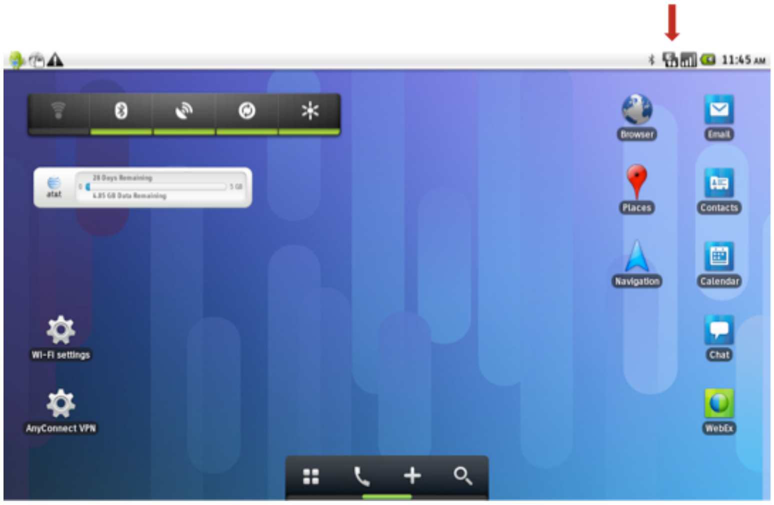
Try to remove the SIM and re-insert it if this icon is displayed.



If currently connected to an HSPA+ (4G) mobile network, then a number of bars will be displayed as well as the H+ icon showing data being transmitted and received.

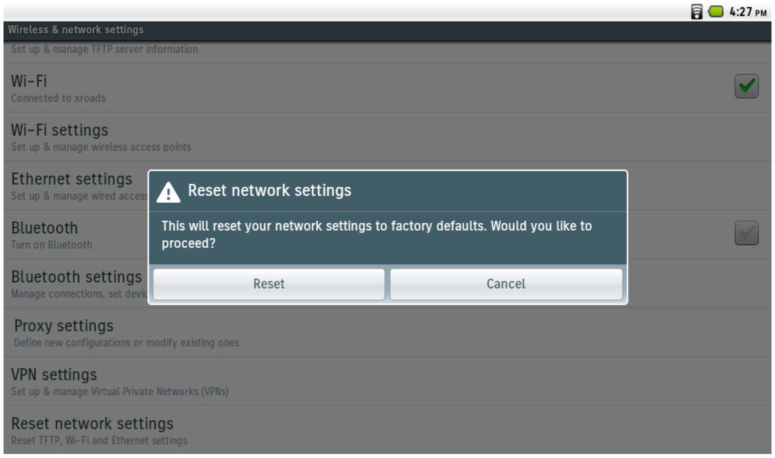


If currently connected to an EDGE (2G) mobile network, then a number of bars will be displayed as well as the E icon showing data being transmitted and received.



Reset Network Settings

Network settings can be reset by selecting **Reset network settings** in Wireless & network settings.



Wireless & network settings

Set up & manage TFTP server information

Wi-Fi
Connected to xroads

Wi-Fi settings
Set up & manage wireless access points

Ethernet settings
Set up & manage wired acces

Bluetooth
Turn on Bluetooth

Bluetooth settings
Manage connections, set devi

Proxy settings
Define new configurations or modify existing ones

VPN settings
Set up & manage Virtual Private Networks (VPNs)

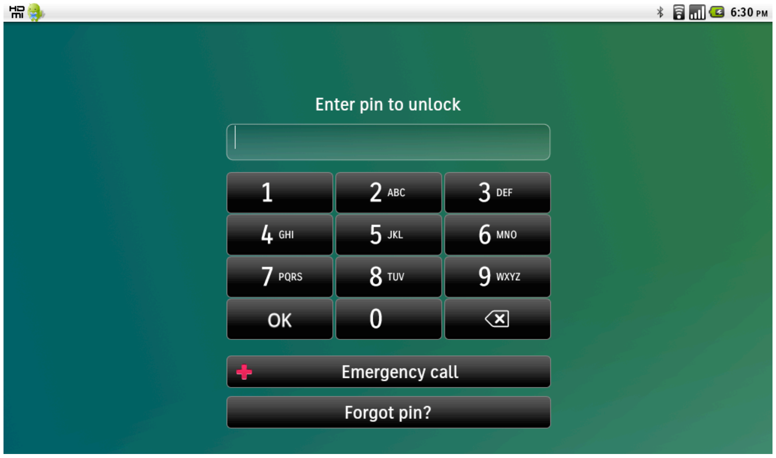
Reset network settings
Reset TFTP, Wi-Fi and Ethernet settings

Reset network settings

This will reset your network settings to factory defaults. Would you like to proceed?

Reset a Forgotten Pin

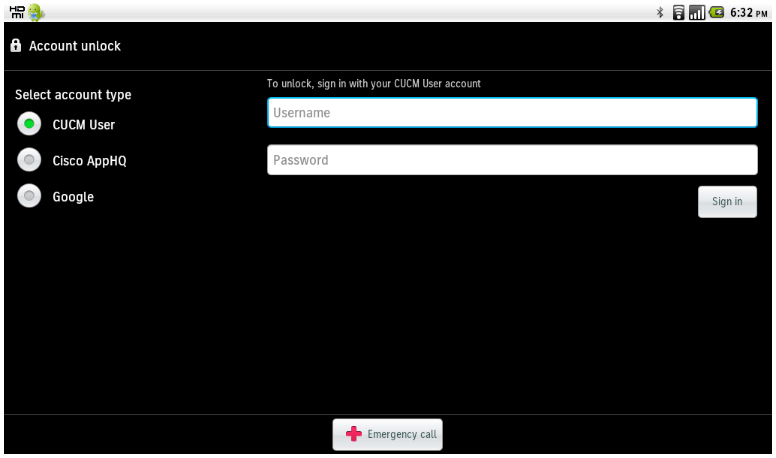
If the pin is forgotten, it can be reset by selecting **Forgot pin?** at the unlock screen.



After **Forgot pin?** is selected, a screen to authenticate via one of the following accounts will be displayed.

- CUCM User
- Cisco AppHq
- Google

When the authentication is successful, the pin can then be reset.


6:32 PM

Account unlock

Select account type

● CUCM User

○ Cisco AppHQ

○ Google

To unlock, sign in with your CUCM User account

Username

Password

Sign in

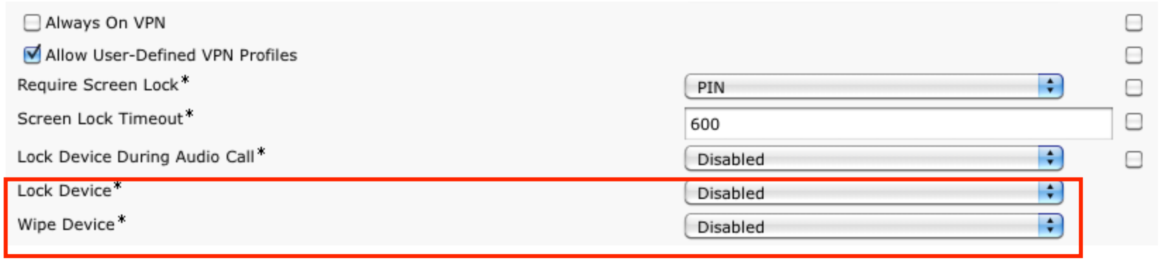
Emergency call

Remote Lock and Wipe

The **Lock Device** option can be enabled if the administrator wants to lock Cisco Cius remotely, which can force the user to enter their pin to gain access to Cisco Cius.

The **Wipe Device** option can be enabled if the administrator wants to erase all the data on Cisco Cius remotely.

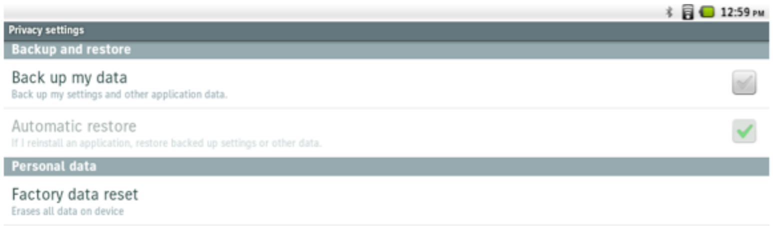
Enabling **Always on VPN** can help to ensure that Cisco Cius SP is always online in order to lock or wipe the device.


□ Always On VPN		□
☑ Allow User-Defined VPN Profiles		□
Require Screen Lock*	PIN	□
Screen Lock Timeout*	600	□
Lock Device During Audio Call*	Disabled	□
Lock Device*	Disabled	
Wipe Device*	Disabled	

Restoring Factory Defaults

All data can be erased from Cisco Cius, by selecting **Factory data reset** in Privacy settings..

A confirmation screen will appear where **Reset phone** must be selected to proceed with the factory data reset.


12:59 PM

Privacy settings

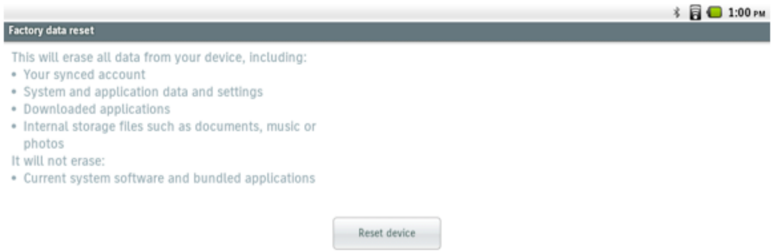
Backup and restore

Back up my data ☑
Back up my settings and other application data.

Automatic restore ☑
If I reinstall an application, restore backed up settings or other data.

Personal data

Factory data reset
Erases all data on device



Factory data reset

This will erase all data from your device, including:

- Your synced account
- System and application data and settings
- Downloaded applications
- Internal storage files such as documents, music or photos

It will not erase:

- Current system software and bundled applications

If Cisco Cius is not able to boot properly, a factory reset can also be initiated via the following procedure:

- Turn the device off by pressing and holding the power button down.
- Press and hold the **Back** and **Menu** keys while powering on Cisco by pressing and releasing the power button while keeping the **Back** and **Menu** keys held down.
- When the red LED begins to flash beside the front camera, release the **Back** and **Menu** keys, and alternate pressing the **Volume Up** and **Volume Down** keys three. This process must be completed within 10 seconds or the factory reset process will be aborted.
- If successful, the LED will remain lit red for approximately 30-45 seconds indicating that Cisco Cius is being reset to factory defaults.
- Cisco Cius will then continue the normal boot process and have the factory settings restored.

Device Debugging

Device debugging can optionally be enabled by accessing Cisco Cius via SSH or Android Debug Bridge (ADB) shell.

If wanting to use ADB, ensure it is enabled in the Cisco Cius configuration within Cisco Unified Communications Manager. Download the Android SDK, which contains ADB from the following location.

http://developer.android.com/sdk

If wanting to use SSH, ensure a username and password are configured in the SSH section of the Cisco Cius configuration within Cisco Unified Communications Manager.
The local login = cisco and the password = default.

Capturing a Screenshot of the Device Display

The current display can be captured by browsing to http://x.x.x.x/CGI/Screenshot, where **x.x.x.x** is the IP address of Cisco Cius. At the prompt enter the username and password for the account that Cisco Cius is associated to in Cisco Unified Communications Manager.

Healthcare Environments

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

Accessories

The following accessories are available for Cisco Cius.

- HD Media Station
- Charging Dock
- Carrying Case
- Jawbone ICON for Cisco Bluetooth Headset

For more information on Jawbone ICON for Cisco Bluetooth Headset, refer to the following URL:
http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10655/ps11204/C78-615196-00_Jawbone_ICON_Cisco_Bluetooth_Headset_DS.pdf

3rd Party Accessories

- Bluetooth Headsets www.plantronics.com
  www.jawbone.com
  www.jabra.com
  www.motorola.com

Additional Documentation

Cisco Cius Data Sheet

http://www.cisco.com/en/US/products/ps11156/products_data_sheets_list.html

Cisco Cius Administration Guide

http://www.cisco.com/en/US/products/ps11156/prod_maintenance_guides_list.html

Cisco Cius User Guide

http://www.cisco.com/en/US/products/ps11156/products_user_guide_list.html

Cisco Cius Release Notes

http://www.cisco.com/en/US/products/ps11156/prod_release_notes_list.html

Cisco Cius Software

http://software.cisco.com/download/navigator.html?mdfid=283319885

Cisco Unified Communications Manager

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Voice Software

http://software.cisco.com/download/navigator.html?mdfid=278875240

Cisco Unified Communications SRND

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html

Cisco Unified Wireless LAN Controller Documentation

http://www.cisco.com/en/US/partner/products/ps10315/products_installation_and_configuration_guides_list.html

Cisco Autonomous Access Point Documentation

http://www.cisco.com/en/US/partner/docs/wireless/access_point/12.4.25d.JA/Configuration/guide/cg_12_4_25d_JA.html