

Configure 802.11n on the WLC

[TAC Notice: What's Changing on TAC Web](#)

Contents

- [Introduction](#)
- [Prerequisites](#)
 - [Requirements](#)
 - [Components Used](#)
 - [Related Products](#)
 - [Conventions](#)
- [802.11n - An Overview](#)
 - [How Does 802.11n Provide Greater Throughput](#)
 - [Guidelines for 802.11n Deployment](#)
- [Configuring 802.11n](#)
 - [Configure the WLC for 802.11n](#)
 - [Configure the Client for 802.11n](#)
- [Factors that Affect 802.11n Throughput](#)
- [Verify](#)
- [Troubleshoot](#)
 - [Unable to Achieve 802.11n Data Rates](#)
 - [Clients Cannot Connect to the WLC](#)
- [NetPro Discussion Forums - Featured Conversations](#)
- [Related Information](#)

Help us help you.

Please rate this document.

Excellent

Good

Average

Fair

Poor

This document solved my problem.

Yes

No

Just browsing

Suggestions for improvement:

(256 character limit)

Introduction

This document provides information on how 802.11n technology works and how to configure 802.11n on the Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How to configure a WLC for basic operations
- Lightweight Access Point Protocol (LWAPP)

Components Used

The information in this document is based on these software and hardware versions:

- WLC 4404 that runs software version 5.1.151.0
- Cisco Aironet 1250 series Access Point (AP)
- Intel Wireless client card adapter

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardware and software versions:

- Cisco 2100 series WLC
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750 Series Integrated WLCs
- Cisco WLC Module

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

802.11n - An Overview

Wireless networks are widely deployed in industrial and domestic environments. New applications are emerging to meet customer needs. Many of these applications are bandwidth intensive. Multimedia applications require more bandwidth for improved performance. 802.11n addresses these challenges by providing throughput as high as 600 Mbps. It also provides better reliability and coverage when compared to existing 802.11 a/b/g technology. This document provides an overview of how 802.11n works and how to configure 802.11n on a WLC.

802.11n can operate either in 2.4 or 5 GHz. They are interoperable with existing 802.11a or 802.11 b/g technologies. This section provides an overview of how 802.11n works. Currently, 802.11n is supported in Cisco 1250 series APs and Cisco 1140 series APs.

How Does 802.11n Provide Greater Throughput

Various techniques are employed in 802.11n to provide higher data rates and better coverage. This section details the techniques used.

MIMO: In the existing 802.11 a or 802.11 b/g technologies, transmission and reception of data streams usually happen using only one of the antennas. However, in 802.11n data streams can be transmitted and received over both the antennas. This results in a greater number of bits transmitted and received at a

given point of time, effective usage of multipath signals which is usually a problem in indoor coverage. This leads to increased throughput and wider coverage. [Table 1](#) shows the data rates of 802.11n currently supported by Cisco¹. **MCS 0-7** are the data rates achieved using single spatial stream (data bits). **MCS 8-15** are the data rates achieved using 2 spatial streams, one over each antenna. Note that the data rates are doubled from 8-15. These data rates (0-15) are described as **MCS rates** throughout this document.

Note: ¹Further higher data rates are planned for future deployments.

Channel Bonding: The amount of data that can be transmitted also depends on the width of the channel used in data transmission. By bonding or combining two or more channels together, more bandwidth is available for data transmission. In 2.4 and 5 GHz frequency band, each channel is approximately 20 MHz wide. In 802.11n, two adjacent channels, each of 20 MHz are bonded to get a total bandwidth of 40 MHz. This provides increased channel width to transmit more data. Cisco does not support channel bonding in 2.4 GHz frequency (802.11 b/g), because only three non-overlapping channels 1, 6 and 11 are available. However, the channel bonding has more relevance in 5 GHz frequency range where you have as many as 23 adjacent non-overlapping channels currently available. Channel bonding is supported only in 5 GHz, for example 802.11a. [Table 2](#) shows the data rates achieved through channel bonding.

Frame Aggregation with A-MPDU: In 802.11, after transmission of every frame, an idle time called **Interframe Spacing (IFS)** is observed before transmitting the subsequent frame. In 802.11n, multiple packets of application data are aggregated into a single packet. This is called **A-MPDU (Aggregated - MAC Protocol Data Unit)**. This reduces the number of IFS, which in turn provides more time for data transmission. In addition, clients operating in 802.11n send acknowledgement for block of packets instead of individual packet acknowledgement. This reduces the overhead involved in frame acknowledgements and increases the overall throughput.

Decreased Timers: In 802.11n, few timers have been reduced to decrease the idle time between individual frame transmissions.

1. **Guard Interval (GI):** In 802.11, data is transmitted as individual bits. A certain amount of time interval is observed before the next bit is transmitted. This is called Guard Interval. GI ensures that bit transmissions do not interfere with one another. As long as the echoes fall within this interval, they will not affect the receiver's ability to safely decode the actual data, as data is only interpreted outside the guard interval. By reducing this interval, data bits are transmitted in shorter intervals and provide for increased throughput.

[Table 1](#) shows how data rates differ based on the Guard Interval for a channel width of **20 MHz**.

Table 1

Modulation Coding Scheme (MCS) Index	MCS Data rates	Modulation used	Data Rate when GI=800ns	Data Rate when GI=400ns
0	1	BPSK	6.5	7 2/9
1	1	QPSK	13	14 4/9

2	1	QPSK	19.5	21 2/3
3	1	16-QAM	26	28 8/9
4	1	16-QAM	39	43 1/3
5	1	64-QAM	52	57 7/9
6	1	64-QAM	58.5	65
7	1	64-QAM	65	72 2/9
8	2	BPSK	13	14 4/9
9	2	QPSK	26	28 8/9
10	2	QPSK	39	42 4/3
11	2	16-QAM	52	57 7/9
12	2	16-QAM	78	86 2/3
13	2	64-QAM	104	115 5/9
14	2	64-QAM	117	130
15	2	64-QAM	130	144 4/9

Table 2 shows how data rates differ based on the Guard Interval for a channel width of **40 MHz**.

Note: You can see that data rates are doubled from MCS 8 - MCS 15.

Table 2

Modulation Coding Scheme (MCS) Index	Number of spatial streams	Modulation used	Data Rate when GI=800ns	Data Rate when GI=400ns
0	1	BPSK	13.5	15
1	1	QPSK	27	30
2	1	QPSK	40.5	45
3	1	16-QAM	54	60
4	1	16-QAM	81	90
5	1	64-QAM	108	120
6	1	64-QAM	121.5	135
7	1	64-QAM	135	157.5
8	2	BPSK	27	30
9	2	QPSK	54	60
10	2	QPSK	81	90
11	2	16-QAM	108	120

12	2	16-QAM	162	180
13	2	64-QAM	216	240
14	2	64-QAM	243	270
15	2	64-QAM	270	300

2. **IFS:** IFS is less in 802.11n when compared to 802.11.

Guidelines for 802.11n Deployment

Keep these guidelines in mind when you deploy 802.11n:

1. Use QoS for LWAPP packets to ensure APs do not lose heartbeats with the controller due to a heavy load added by 802.11n.
2. LAPs can be powered using a local power supply, power injector or an 802.3af capable switch. **1140 series APs** are easy to deploy as these APs can be fully powered using the existing **802.3af standard**. However, in 1250 series APs, dual-band products (APs with both 802.11b/g/n and 802.11a/n radios) cannot be fully powered by 802.3af and require 802.3at or a power injector to operate both transmitters in each band. 802.3af can either support both transmitters on an AP with a single radio (either 802.11b/g/n or 802.11a/n), or 802.11n with a single transmitter in each band (802.11b/g/n and 802.11a/n).

Note: M8 to M15 data rates are disabled because they require both transmitters in the band to be operational.

3. 1250 series APscan support 802.11n with reduced power (11 dBm) for both transmitters in each band (802.11b/g/n and 802.11a/n).
 - a. Requires Cisco switches with Enhanced POE (16.8W) and CDP.
 - b. M0 to M15 data rates are reduced due to reduced power but are still enabled.
4. Use only 20 MHz 802.11n mode in 2.4 GHz. Cisco supports both 20 MHz and 40 MHz (Channel bonding) 802.11n mode only in 5GHz..
5. Use 20 MHz (Non-Channel Bonding) in 5 GHz (802.11 a/n) when:
 - a. Voice traffic is using 802.11a
 - b. 20 MHz is better in mixed .11a and .11n environments
6. Use 40 MHz (Channel Bonding) in 5 GHz (802.11a/n) when:
 - a. Traffic uses heavy bandwidth (video)
 - b. 40 MHz is better when most clients are 802.11n

Configuring 802.11n

Configure the WLC for 802.11n

This section shows how to configure the 5 GHz frequency band on the WLC for 802.11n support. Complete these steps:

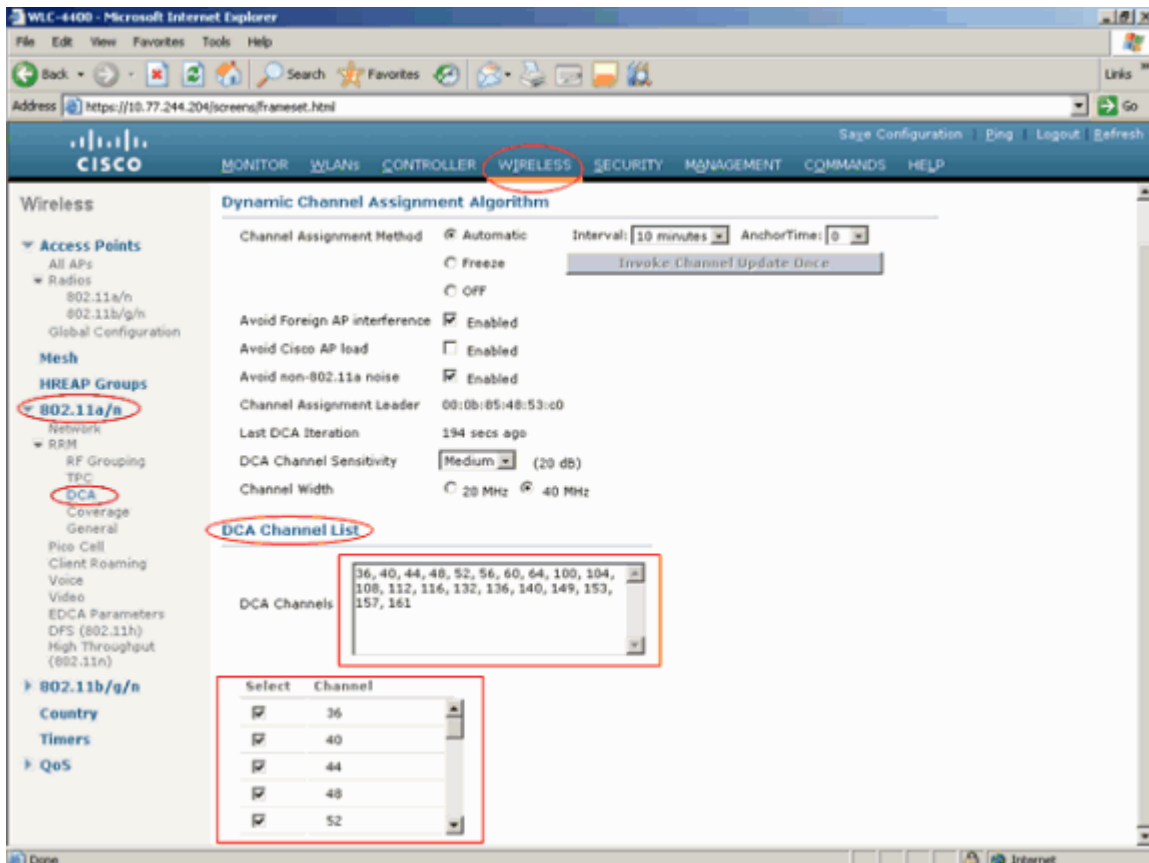
Note: These steps are similar for 2.4 GHz frequency band except that occurrences of 802.11a should be replaced with 802.11 b/g.

1. Enable the 802.11n support on the 802.11a network.

```
(Cisco Controller)>config 802.11a 11nsupport enable
```

Note: Before you enable 802.11n support, the 802.11a network needs to be disabled.

2. 802.11n operates on the same channel as 802.11a. For better compatibility with 802.11n clients, it is recommended to stay on lower channels (UNII-1 band). Check the list of channels used in channel allocation for APs from the **DCA Channel List** menu under **Wireless > 802.11a/n > DCA** on the WLC GUI. In order to include or delete a channel from the list, use the **Select Channel** list.



3. You can also manually configure the channel for an individual lightweight access point (LAP). This helps to control the channel in an environment where only 802.11n clients connect. This

makes troubleshooting easier. Use this command:

```
(Cisco Controller) >config 802.11a channel AP001b.d4e3.a81b 36
!--- Sets 802.11a channel to 36 on AP AP001b.d4e3.a81b.
```

4. Channel bonding in 802.11a provides twice the normal throughput. You bind a channel with the next adjacent channel in the frequency domain. This is an example of channel bonding. Here the channel **36** is bonded with the adjacent channel to provide a channel width of 40 MHz.

```
(Cisco Controller)> config ap <AP Name>
(Cisco Controller)> config 802.11a disable <Ap name>
(Cisco Controller)> config 802.11a channel <Ap name> 36
Set 802.11a channel to 36 on the specified AP.
(Cisco Controller)> config 802.11a txpower <Ap name> 1
Sets power on the AP.
(Cisco Controller)> config 802.11a chan_width <Ap name>
40
Here you have an option of configuring channel width
(Cisco Controller)> config 802.11a enable <Ap name>
(Cisco Controller)> config ap enable <Ap name>
```

In order to check if this has worked, use the **show ap config 802.11a <ap name>** command. This command shows the list of parameters that are specific to 802.11a. The **Extension channel** field under the PHY OFDM parameters displays the channel bonded to the *Current operating channel* of the AP.

5. Use these commands to configure the features that are specific to 802.11n:

```
(Cisco Controller) >config 802.11a 11nSupport a-mpdu tx priority <0-7/all>
(This enables the aggregation of frames(A-MPDU) for the traffic of

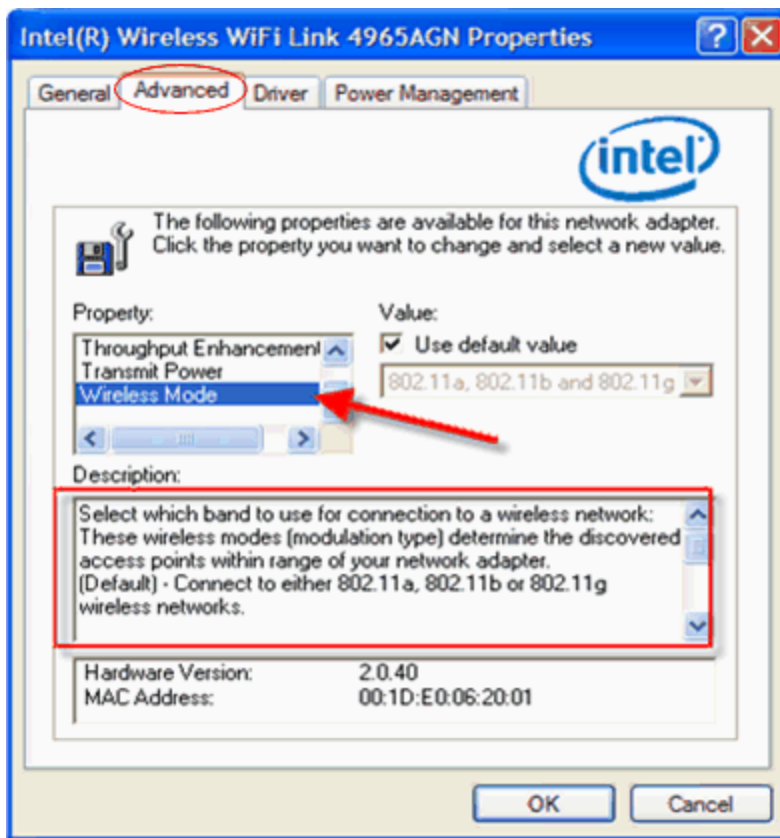
(Cisco Controller) >config 802.11a 11nSupport mcs tx <0-15>
(This configures the 802.11n rates at which data is transmitted b
```

Configure the Client for 802.11n

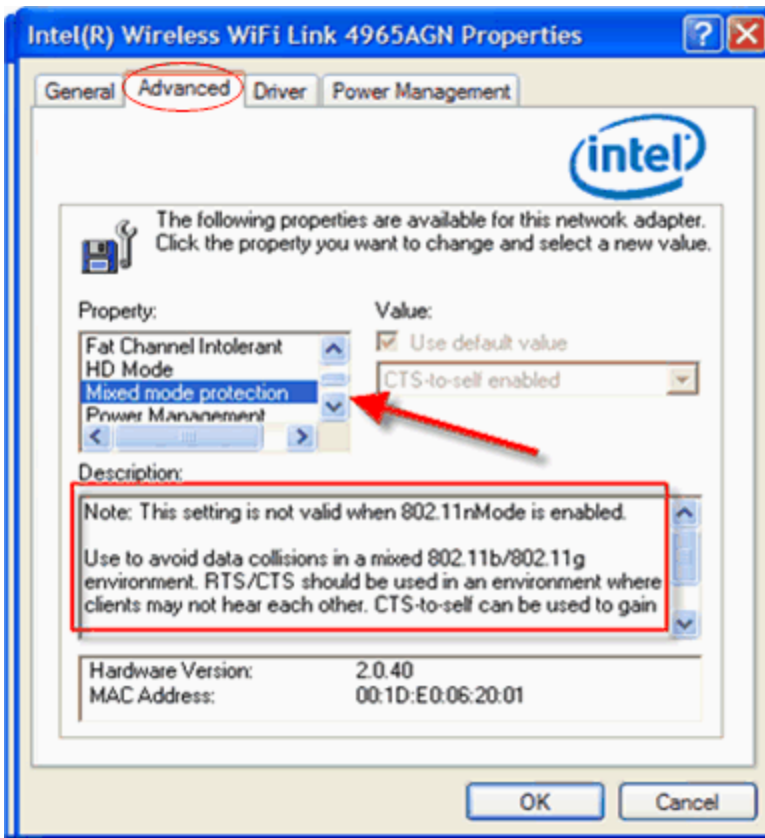
Many of the client cards operate in 2.4 GHz. Make sure you use the client card that supports 5 GHz to make use of channel bonding.

These steps show how to configure an Intel Card for 802.11n on an XP machine:

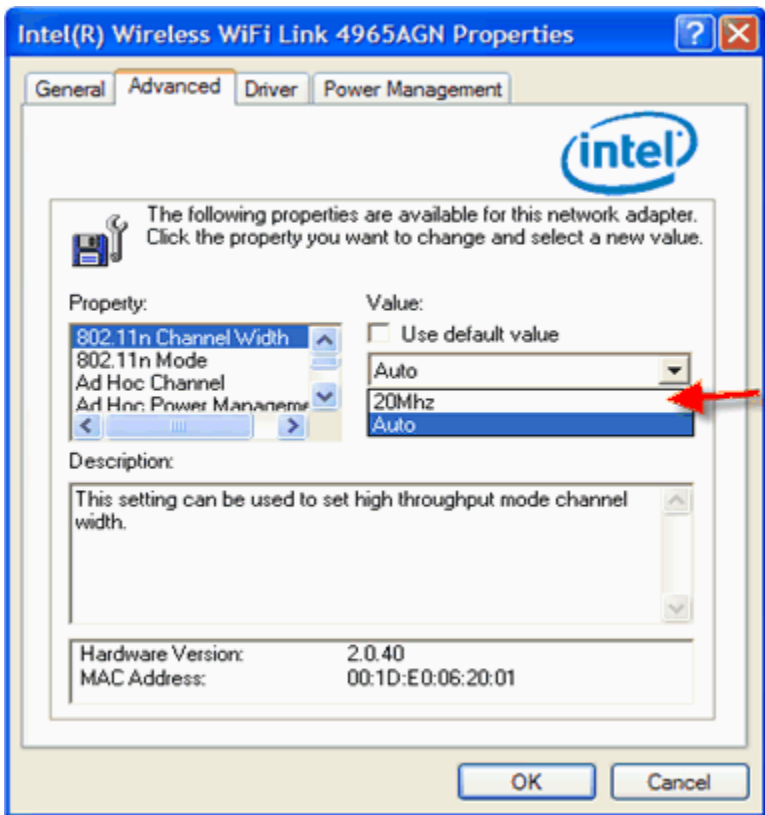
1. Click the **Start** menu. Go to **Settings** and choose **Control Panel**.
2. Double-click the **Network Connections** icon.
3. Right-click the Intel Wireless Card and click **Properties**.
4. Click the **Advanced** tab.
5. Choose the *Use the default value* option for the Wireless Mode property so the client can operate either in 802.11a mode or in 802.11 b/g mode, whichever is available.



6. Unless the network is comprised only of 802.11n clients, use **Mixed mode protection** so the 802.11n clients coexist with existing 802.11a or 802.11 b/g clients.

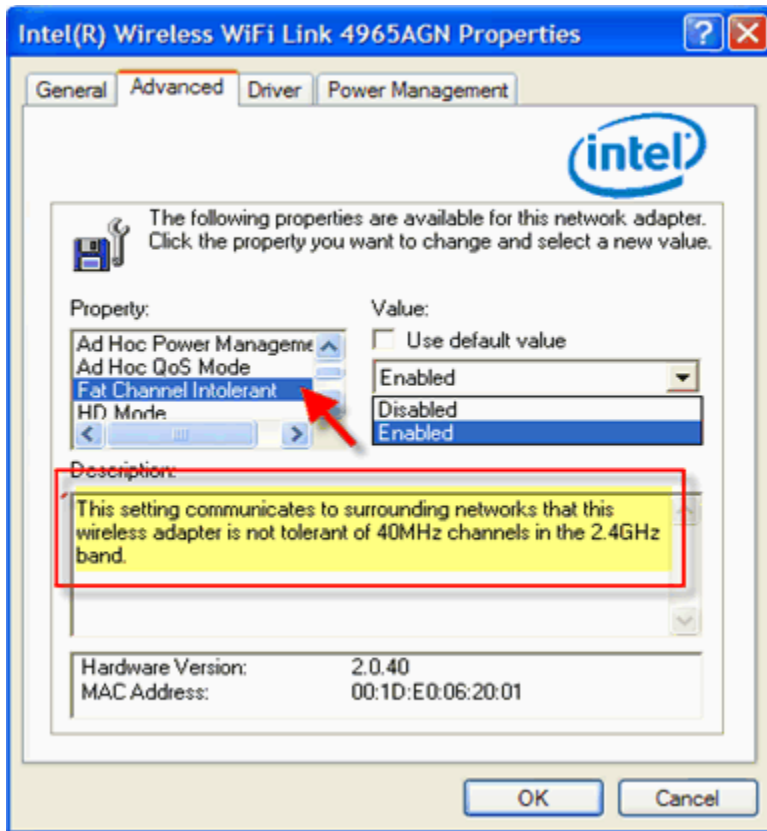


7. Set the Channel Width either in Auto mode so the client negotiates the channel width with the WLC, or in 20 MHz if it is 2.4 GHz frequency band.



Note: Cisco supports 40 MHz only in 5 GHz band. Set the channel width option to **Auto** to make use of 40 MHz channel width. However, make sure 40 MHz channel width is enabled on the WLC.

8. Disable the **Fat Channel Intolerant** property to allow 40 MHz Channel Bonding.



Factors that Affect 802.11n Throughput

There are circumstances where 802.11n devices cannot operate at their maximum capable data rates. There are various reasons why this occurs. This is the list of factors that affect 802.11n throughput:

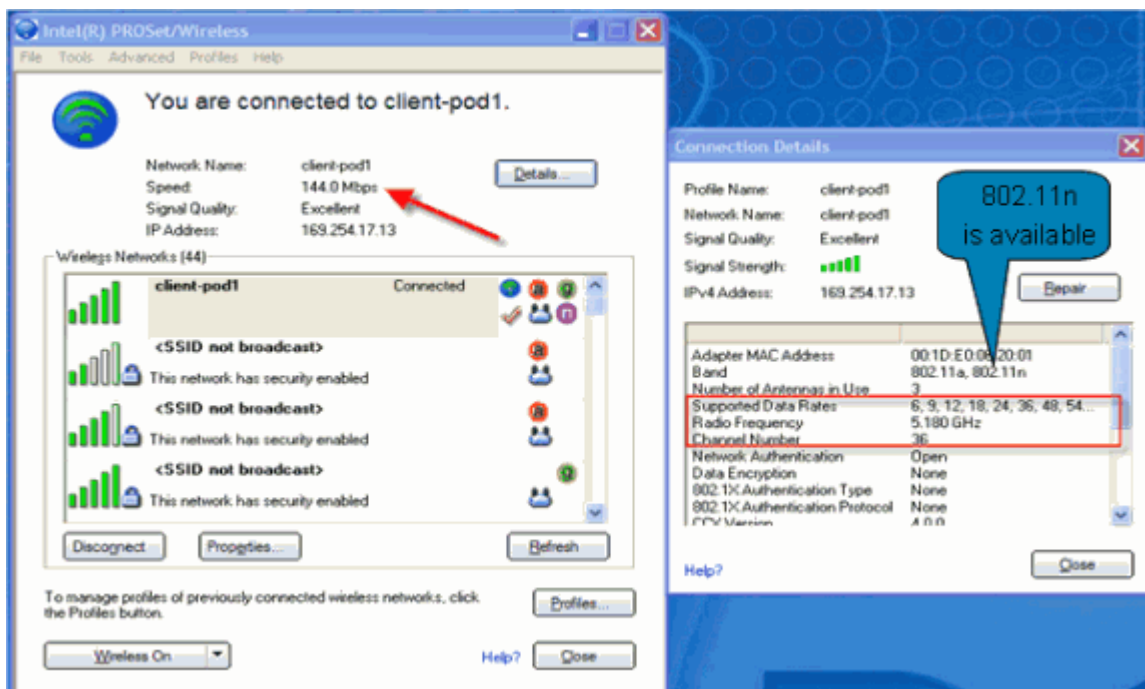
1. When 802.11n clients operate in a mixed environment with 802.11a or 802.11 b/g clients, 802.11n provides a protection mechanism to interoperate with 802.11a or 802.11 b/g clients. This introduces an overhead and reduces the throughput of 802.11n devices. Maximum throughput is achieved in **Greenfield mode** where only 802.11n clients exist.
2. Factors such as Channel width, Guard Interval and Reduced IFS (RIFS) play a major role in the bandwidth. [Table 1](#) and [Table 2](#) show how these factors affect the bandwidth.
3. Clients ability to send a Block Ack instead of individual frame acknowledgements.
4. MCS Index configured on the WLC.
5. Proximity to AP—Clients closer to the AP experience higher data rates. As clients move farther away from the AP, signal strength reduces. As a result, data rate decreases steadily.

- RF environment—Amount of noise and interference in the environment. The less the noise and interference, the greater the bandwidth.
- Encryption/ Decryption—Encryption in general reduces the throughput due to the overhead involved in the data encryption/decryption process. However, advanced encryption standards, such as AES, can provide better throughput when compared to other encryption standards, such as TKIP and WEP.
- Wired Network Infrastructure—Bandwidth of the wired infrastructure determines the speed of the traffic to and from the wired network to the wireless clients.

Verify

You can check the connection status, speed, mode and signal strength of a client both from the WLC and the client.

- If you use an Intel client, right-click the **Wireless icon** in the System Tray (bottom right corner of the desktop) in order to view the wireless mode. Then, click **Status** and check the band. In order to check the speed of client operation, right-click the **Wireless icon** and click **View Available Wireless Networks**. Click the SSID and check the speed as shown here:



- On the WLC GUI, click **Monitor**. Then, click **Clients** in the left side. This displays the list of clients currently associated to the WLC. Next, click on a client to check the mode, speed and other details of its connectivity.

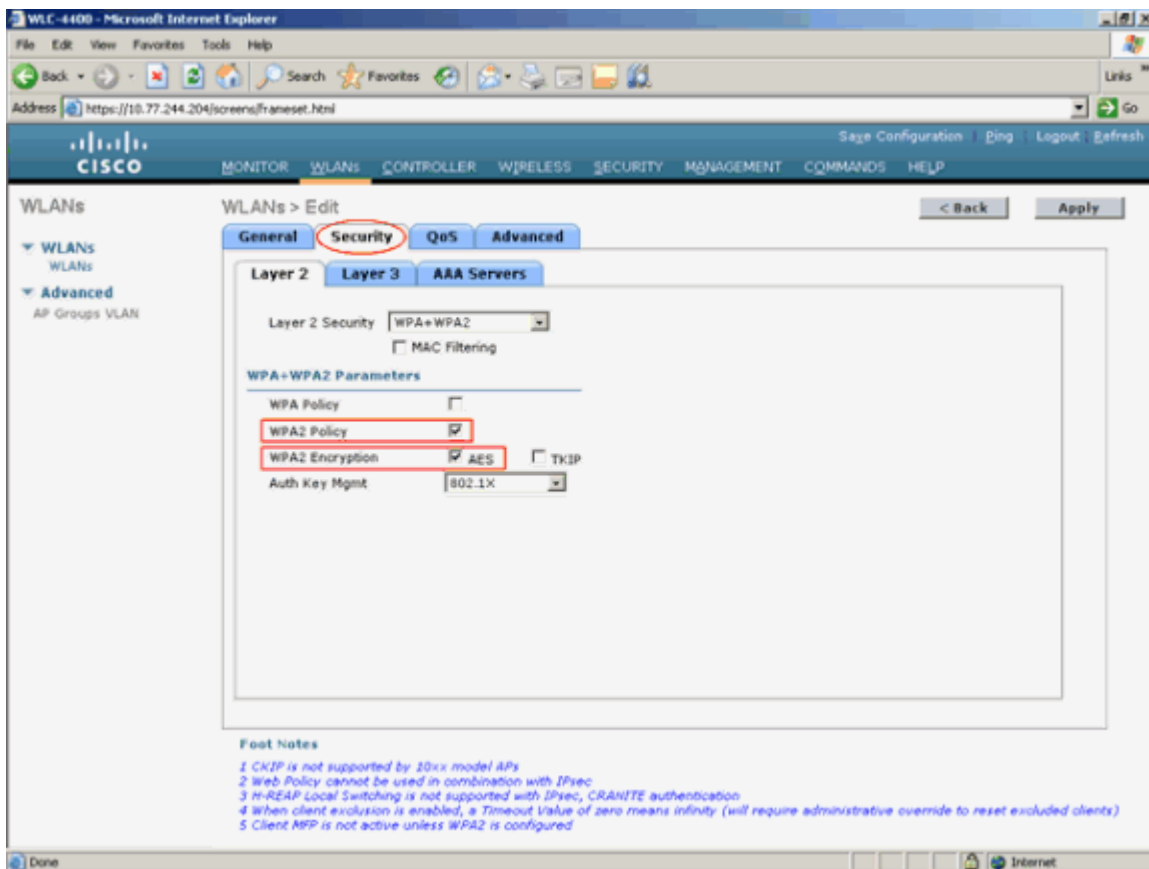
Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:13:ce:f6:3d:d9	API252-0017.94cc.d9f6	Unknown	802.11a	Probing	No	1	No
00:13:ce:c9:25:56	API252-0017.94cc.d9f6	Unknown	802.11a	Probing	No	1	No
00:13:ce:c9:29:2b	API252-0017.94cc.d9f6	Unknown	802.11a	Probing	No	1	No
00:16:a4:0e:8e:8a	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:16:a4:0e:20:01	API252-0017.94cc.d9f6	client-pod1	802.11n(5)	Associated	Yes	1	No
00:40:96:b3:a4:86	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b3:a4:8b	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b3:a4:8d	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b3:a4:8d	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b4:8b:26	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b4:8c:04	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b4:8c:0b	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No
00:40:96:b4:8d:ad	API252-0017.94cc.d9f6	Unknown	802.11b	Probing	No	1	No

Troubleshoot

Unable to Achieve 802.11n Data Rates

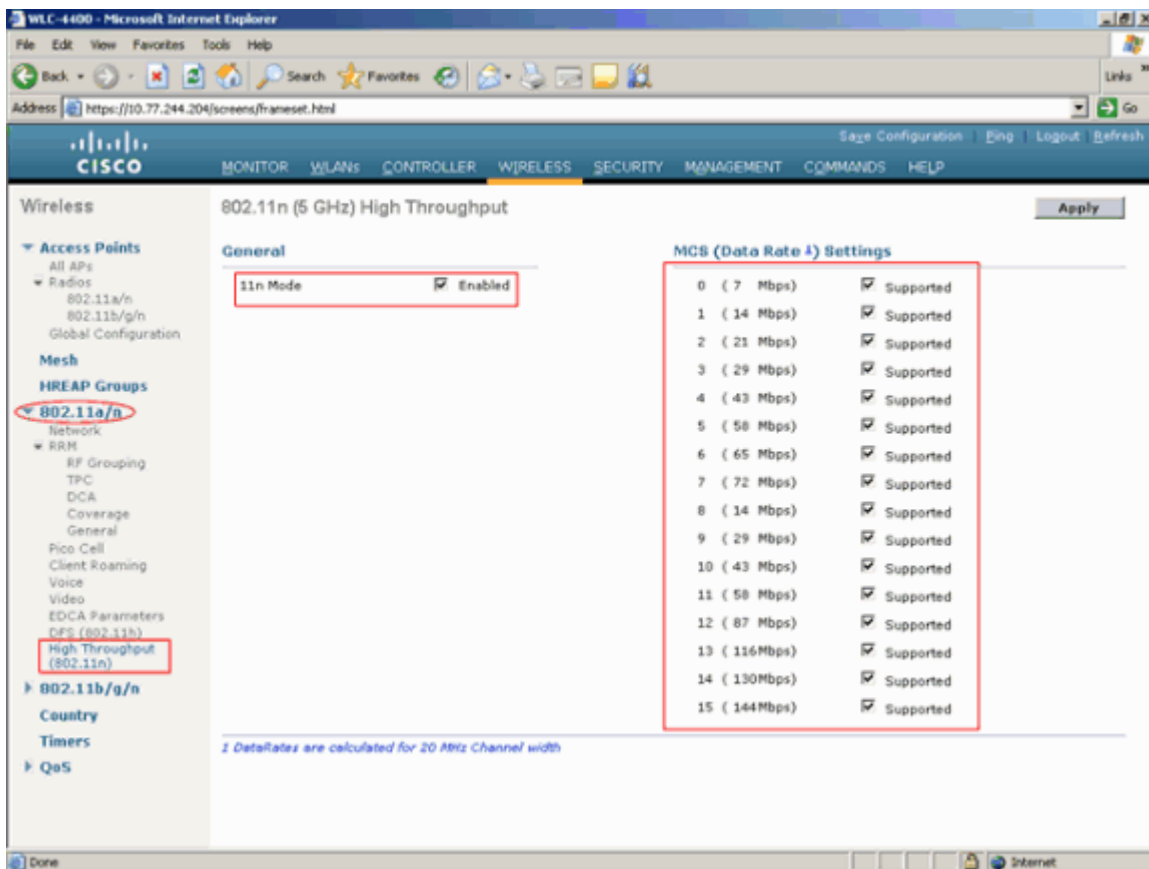
One of the most common issues is that you cannot achieve the maximum throughput in 802.11n. Perform these checks:

1. 802.11n requires AES encryption to be enabled on WLANs used by 802.11n clients. You can use a WLAN with NONE as Layer 2 Security. However, if you configure any Layer 2 security, 802.11n requires WPA2 AES enabled to operate at 11n rates.



Note: If you have legacy clients, you can enable WPA TKIP to provide interoperability.

2. Make sure the AP has enough power. Lower power on the AP results in lower signal strength, which decreases the throughput.
3. Make sure the 802.11n rates are enabled. MCS rates should be enabled (this is recommended to keep all of the MCS rates enabled).

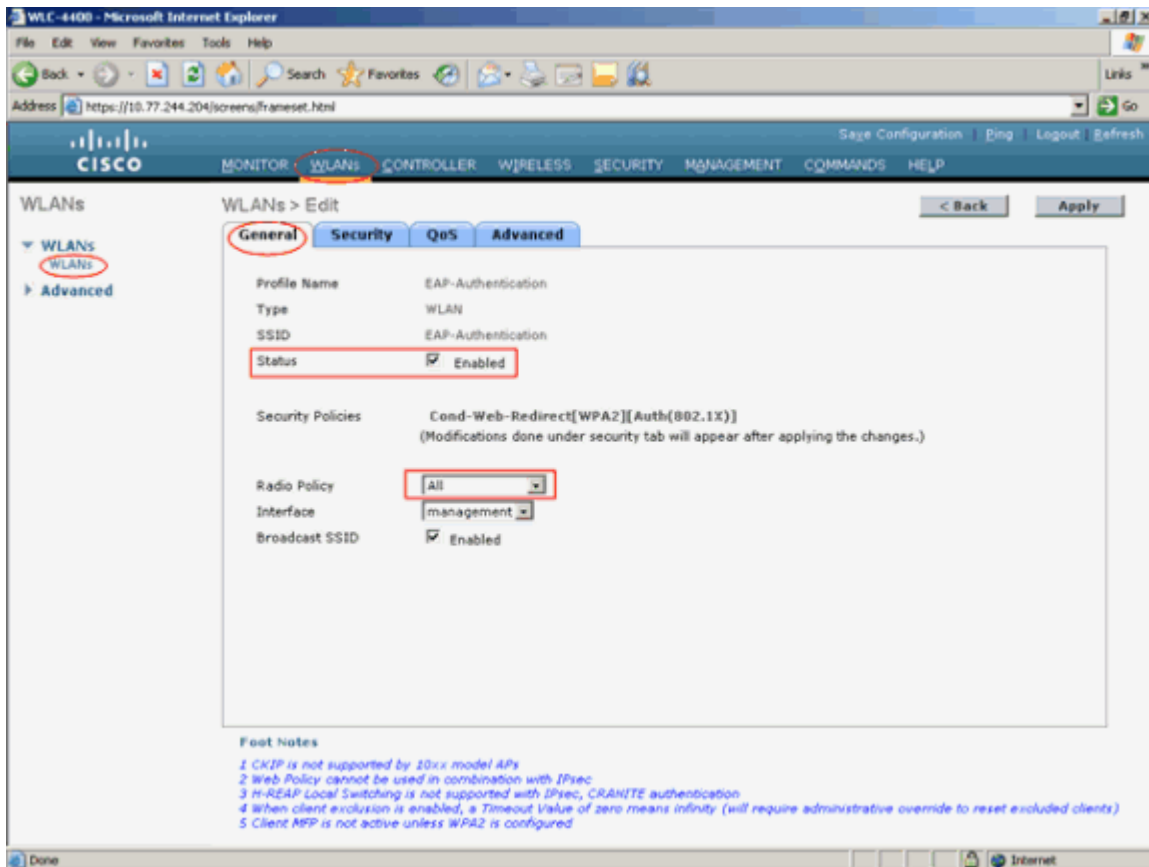


4. Make sure that the AP has 2 external antennas to avail the data rates **MCS 8-15** as shown in the previous figure.
5. Ensure that WMM is set to **Allowed** on the WLAN profile in order to achieve 802.11n rates.

Clients Cannot Connect to the WLC

Issues in 802.11n networks are similar to that of the 802.11 network as far as the connectivity is concerned. Perform these checks:

1. Make sure that the LAP has joined the controller and all radios are up. Check this under **Wireless > All APs**.
2. Make sure that the WLAN is enabled and configured to **All** under Radio Policy in order to operate in both 2.4 GHz and 5 GHz band.



For more information on how to troubleshoot connectivity issues, refer to [Troubleshooting Client Issues in the Cisco Unified Wireless Network](#).

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Wireless
Wireless - Mobility: WLAN Radio Standards
cannot lock rf frequency - May 21, 2009 Encryption on 1131AG - May 21, 2009 Prefer 802.11a over 802.11g - May 20, 2009 4 VLAN enable for Cisco 1100 - May 20, 2009 1300 or 1400 bridge remote setup - May 14, 2009
Wireless - Mobility: Security and Network Management
wlc 4404 and high availability - May 20, 2009 Optional WEP on Autonomous AP1230 - May 20, 2009 WCS Windows Server Rename - May 20, 2009 Sample TAR for passthrough? - May 20, 2009 WLC 4402 : Order of WLAN profiles in an AP group from MIB files - May 20, 2009
Wireless - Mobility: Wireless IP Voice and Video

[Multicast on LWAP AP](#) - May 20, 2009
[WLC AP Fallback Fails with Vlan Tagging](#) - May 19, 2009
[wifi VOIP and 911](#) - May 19, 2009
[7921G not registering with CME 4.0](#) - May 19, 2009
[7921 - intermittently flip to vibrate](#) - May 18, 2009

Wireless - Mobility: Getting Started with Wireless

[521G Access Point Configure Terminal mode via telnet](#) - May 21, 2009
[wifi - INFO REQUEST](#) - May 21, 2009
[1242 downgrade process fails - why?](#) - May 21, 2009
[AP Comparison for site survey](#) - May 21, 2009
[Aironet 1250 and AIR-ANT2430V-R](#) - May 20, 2009

Wireless - Mobility: General

[cannot access 4402 controller management IP](#) - May 21, 2009
[AP disappearing from WLC AP list](#) - May 21, 2009
[Not enough room on Flash when trying to upgrade Firmware on 1200 AP](#) - May 21, 2009
[SSH communication](#) - May 21, 2009
[ap 1520 and devices on poe out.](#) - May 21, 2009

Related Information

- [802.11n Wireless Technology Overview](#)
- [Cisco 802.11n Design and Deployment Guidelines](#)
- [Cisco Wireless LAN Controller Command Reference, Release 5.1](#)
- [Technical Support & Documentation - Cisco Systems](#)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)