



Wi-Fi Cloud

AP Deployment Guide

WatchGuard Wi-Fi Cloud & APs

AP120, AP125, AP225W, AP320, AP322, AP325, AP327X, AP420

About This Guide

The *WatchGuard Wi-Fi Cloud AP Deployment Guide* is a guide to help you with your deployment of a WatchGuard AP with WatchGuard Wi-Fi Cloud. For the most recent product documentation, see the *WatchGuard Wi-Fi Cloud Help* on the WatchGuard website at <https://www.watchguard.com/wgrd-help/documentation/overview>.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 3/30/2023

Copyright, Trademark, and Patent Information

Copyright © 1998-2023 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at <https://www.watchguard.com/wgrd-help/documentation/overview>.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

Introduction to the Deployment Guide	1
Overview.....	2
Current AP Models.....	2
Legacy AP Models.....	3
WatchGuard AP Management.....	3
WatchGuard Wi-Fi Subscriptions.....	4
WatchGuard Wi-Fi Cloud Architecture.....	5
Cloud-based Management with WatchGuard Discover.....	6
Trusted Wireless Environment with WIPS.....	7
WatchGuard Analyze.....	9
Scalable, Multi-Tenant, Elastic Cloud Architecture.....	9
Zero Touch Deployment.....	10
Regulatory Compliance Reports.....	11
Wireless Network Design	12
Evaluate Requirements.....	12
Coverage Planning.....	12
Capacity Planning.....	13
Wireless Site Survey.....	13
Channel Capacity Planning.....	14
Design Wireless Networks for Capacity.....	14
Requirements Analysis – Clients.....	15
Requirements Analysis – Applications.....	16
Use Cases.....	17
Environment Analysis.....	17
Wireless Environmental Factors.....	17
Wireless Regulatory Domain.....	17

RF Environment	17
Channel Capacity Planning	18
Spectrum Availability in 5 GHz	18
802.11ac Wave 1 and Wave 2	19
MU-MIMO	19
DFS Channels	20
Channel Width Selection	21
Estimate Channel Capacity	21
Channel Capacity Estimate Considerations	22
Channel Capacity Calculations	23
Maximum Clients For APs	25
Summary of Channel Capacity Planning Recommendations	26
Site Preparation Checklist	27
Getting Started with WatchGuard Wi-Fi Cloud	29
Getting Started with WIPS	29
Deployment Best Practices	30
Wireless Network Best Practices	31
AP Transmit Power Reduction	31
Fast Roaming	32
802.11k and 802.11v	33
SSID Bridge vs. NAT Mode	34
Smart Client Load Balancing and Steering	35
Smart Steering	35
Band Steering	35
Broadcast/Multicast Control	37
Reliable Multicast Delivery and IGMP Snooping	39
Set a Minimum Unicast Rate	40
Multicast, Broadcast and Management Rate Optimization	41

Traffic Shaping	42
Wi-Fi Multimedia and Quality of Service	43
End-to-End QoS	44
Application Visibility and Control	45
Application Firewall	46
WIPS (Wireless Intrusion Prevention System)	47
Summary of Wireless Network Recommendations	49
Wired Network Best Practices	51
AP Power Requirements	51
AP Uplink Capacity	53
Link Aggregation	53
AP Cabling	53
Access Network Uplink	54
VLAN Design	55
Jumbo Frames	55
Summary of Wired Network Recommendations	56
Network Services Best Practices	57
AP Placement and Channel Plan Best Practices	59
Wireless Signal Strength and Noise Levels	59
Signal Strength	59
Noise Level	59
Signal to Noise Ratio	59
RF Interference	60
Wi-Fi Interference Sources	60
Non-Wi-Fi Interference Sources	60
Microsoft Xbox Game Controller	60
Microwave Oven	61
Bluetooth	61

Wi-Fi Cloud Smart Spectrum	62
Spectrum Analysis with Discover	62
Signal Strength, Channel Width, and QAM	62
Predictive Site Survey	64
Indoor Attenuation Reference	65
Rule of 10s and 3s	66
One-for-One AP Replacement	67
Avoid Self Induced CCI in 2.4 GHz	67
40 MHz Channel Plan	67
80 MHz Channel Plan	68
AP Mounting Recommendations	69
Wall Mount	69
Ceiling Mount	69
Structural Proximity and Electrical Interference	70
AP Placement	71
Post-Deployment Validation Survey	72
Summary of Recommendations for an AP Placement and Channel Plan	73
Deployment Use Cases	75
Use Case 1 – Classroom	75
Requirements	75
Environment	75
Channel Capacity Planning	75
Step 1	76
Step 2	76
Solution	77
5 GHz Plan	77
2.4 GHz Plan	78
Use Case 2 – Lecture Hall	79

Requirements	79
Environment	79
Channel Capacity Planning	79
Step 1	79
Step 2	80
Solution	81
5 GHz Plan	82
2.4 GHz Plan	83
Use Case 3 – Dormitories	84
Requirements	84
Environment	84
Channel Capacity Planning	84
Step 1	84
Step 2	85
Solution	85
5 GHz Plan	86
2.4 GHz Plan	87
Channel Capacity Estimates	88

Introduction to the Deployment Guide

This guide provides best practices for network design, deployment, and configuration of enterprise wireless environments with WatchGuard Wi-Fi Cloud.



This guide applies to Wi-Fi Cloud-managed Access Points (AP120, AP125, AP225W, AP320, AP322, AP325, AP327X, AP420)

This guide includes these topics:

- [Overview](#)
- [Wireless Network Design](#)
- [Getting Started with WatchGuard Wi-Fi Cloud](#)
- [Deployment Best Practices](#)
 - [Wireless Network Best Practices](#)
 - [Wired Network Best Practices](#)
 - [Network Services Best Practices](#)
 - [AP Placement and Channel Plan Best Practices](#)
- [Deployment Use Cases](#)






This guide is intended for use by engineers with a background in wireless technology and for those involved with design, installation, and optimization of WatchGuard wireless networks.

Overview

The WatchGuard AP family of wireless access points provide secure, reliable, wireless communications while delivering high performance and broad coverage to meet the needs of enterprise-level customers, small businesses, branch offices, campuses, and hotels.

Internal antennas, slim cases, minimalist labeling, and small LEDs, coupled with wall and ceiling mount options and Power over Ethernet (PoE) make these devices ideal for low profile deployment scenarios.

Current AP Models

					
Recommended Use Case	AP125 Lower-density high performance ideal for small schools, distributed remote offices, and small meeting rooms	AP225W Medium-density high performance ideal for multi-dwelling units (MDU) structures such as dorm rooms, hotels, assisted living, and military housing units.	AP325 Medium-density high performance including K-12 schools, SMBs, restaurants	AP327X Medium-density high performance IP-67 rated rugged outdoor including school campuses, RV parks, manufacturing yards, warehouses	AP420 High-density, high performance including large schools, meeting rooms, shopping malls
Radios & Streams	2x2:2 MU-MIMO Wave 2	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2 3rd WIPS Radio	2x2:2 MU-MIMO Wave 2	4x4:4 MU-MIMO Wave 2 3rd WIPS radio
Deployment	Indoor	Indoor	Indoor	Outdoor	Indoor
Number of Antennas	4 Internal	4 Internal	6 Internal	4 N-Type External Connectors	10 Internal
Maximum Data Rate	867 Mbps/300 Mbps	867 Mbps / 400 Mbps	867 Mbps/300 Mbps	867 Mbps/400 Mbps	1.7 Gbps/800 Mbps
Ports	2x Gbe	3x Gbe	2x Gbe	2x Gbe	2x Gbe
Power over Ethernet (PoE)	802.3af (PoE)	802.3at (PoE+)	802.3at (PoE+)	802.3at (PoE+)	802.3at (PoE+)
Product Dimensions	5.83" x 5.83" x 1.29" (148 x 148 x 33 mm)	7.3" x 4.9" x 1" (186.4 x 123.9 x 25.5mm)	7.72" x 7.72" x 1.69" (196 x 196 x 43 mm)	8.42" x 8.42" x 2.66" (213.9 x 213.9 x 67.5 mm)	8.66" x 8.66" x 2.24" (220 x 220 x 57 mm)

Legacy AP Models

Legacy AP Models	AP120	AP320	AP322
Recommended Use Cases	Low-density	Medium-High Density	High performance rugged outdoor
Radios and Streams	2x2 MIMO Wave 1	3x3 MIMO Wave 1	3x3:3 MIMO Wave 1
Deployment	Indoor	Indoor	Outdoor
Number of Antennas	4 internal	6 internal	6 internal
Maximum TX Power	20 dBm	20 dBm	20 dBm
Maximum Data Rate (5 GHz / 2.4 GHz)	867 Mbps / 300 Mbps	1.3 Gbps / 450 Mbps	1.3 Gbps / 450 Mbps
Ports	2x GbE	2x GbE	2x GbE
Power	802.3af (PoE)	802.3af (PoE)	802.3at (PoE+)

WatchGuard AP Management

There are two ways you can manage WatchGuard APs:

WatchGuard Firebox Gateway Wireless Controller

This management solution provides local management, configuration, security, and monitoring of APs directly from your WatchGuard Firebox with the Gateway Wireless Controller.

WatchGuard Wi-Fi Cloud

WatchGuard Wi-Fi Cloud provides a powerful cloud-based enterprise wireless management solution for AP configuration, security, and monitoring. When managed by our WatchGuard Wi-Fi Cloud, WatchGuard APs deliver fast, reliable wireless access and provide industry-leading wireless security, guest engagement, and analytic tools. The solution has also been designed from the ground-up to focus on ease of deployment and administration, to simplify the most complex aspects of Wi-Fi management, and to make fast, secure, and intelligent Wi-Fi accessible to organizations of all types and sizes.

In this guide, we use the powerful features available in WatchGuard Wi-Fi Cloud for the examples and use cases.

WatchGuard Wi-Fi Subscriptions

WatchGuard offers three types of wireless security subscriptions for WatchGuard APs:

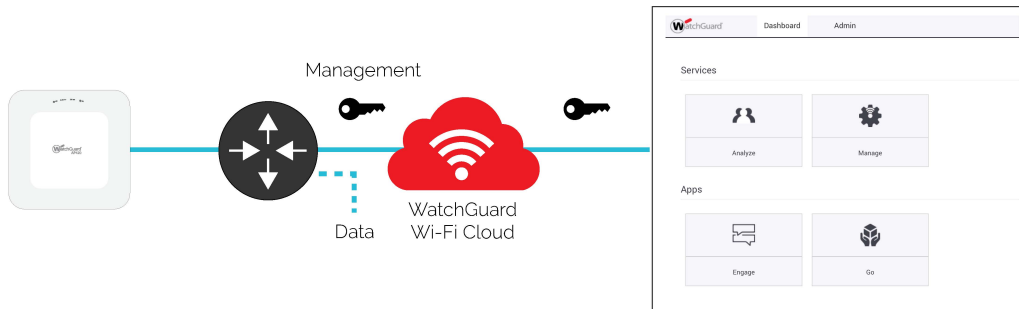
- **Basic Wi-Fi** – Use the Gateway Wireless Controller on a WatchGuard Firebox to configure, manage, and monitor WatchGuard APs directly from the Firebox.
- **Secure Wi-Fi** – Use WatchGuard Wi-Fi Cloud for WatchGuard AP management, security, and monitoring.
- **Total Wi-Fi** – Use WatchGuard Wi-Fi Cloud for WatchGuard AP management, security, and monitoring. With Total Wi-Fi, you also get access to additional tools for guest user engagement, analytics, social media integration, captive portals, and splash page design. You can also create a Trusted Wireless Environment for your users.

WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Management Platform	Wi-Fi Cloud	Wi-Fi Cloud	Firebox Appliance*
Scalability Number of managed access points.	Unlimited	Unlimited	Limited**
Configuration and Management SSID configuration with VLAN support, band steering, smart steering, fast roaming, user bandwidth control, Wi-Fi traffic dashboard.	✓	✓	✓
Additional Wi-Fi Cloud-based Management Radio Resource Management, Hotspot 2.0, enhanced client roaming, nested folders for configuration before deployment, integration with 3rd party WLAN controllers.	✓	✓	
Intelligent Network Visibility and Troubleshooting Pinpoint meaningful network problems and application issues by seeing when an anomaly occurs above baseline thresholds and remotely troubleshoot.	✓	✓	
Verified Comprehensive Security A patented WIPS technology defends your business from the six known Wi-Fi threat categories, enabling a Trusted Wireless Environment.	✓	✓	
GO Mobile Web App Quickly and easily set-up your WLAN network from any mobile device.	✓	✓	
Guest Engagement Tools Splash pages, social media integrations, surveys, coupons, videos, and so much more.	✓		
Location-based Analytics Leverage metrics like footfall, dwell time, and conversion to drive business decisions and create customizable reports.	✓		
Support Hardware warranty with advance hardware replacement, customer support, and software updates	Standard	Standard	Standard

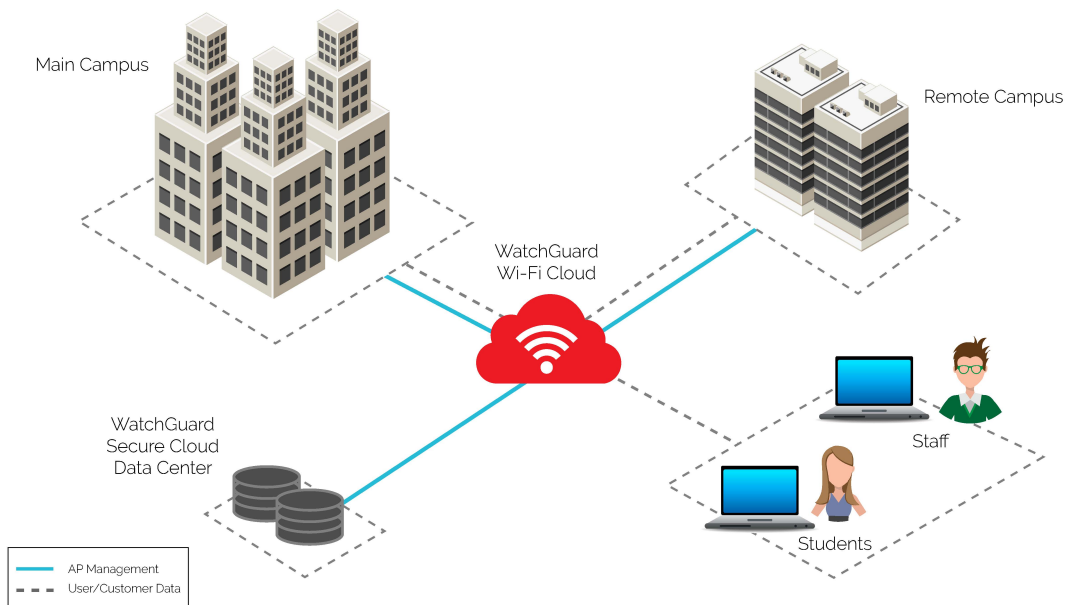
**20 access points recommended for each Firebox model. 4 access points are recommended for the T-15 Firebox model.
*Requires Firebox with active support contract.

WatchGuard Wi-Fi Cloud Architecture

With WatchGuard Wi-Fi Cloud, all services, such as Wi-Fi, WIPS, monitoring, troubleshooting, and guest management, are integrated into a single cloud platform. This provides a cost-effective, easy to manage, highly scalable, secure and reliable cloud Wi-Fi solution.



The Wi-Fi Cloud solution is built on a controller-less architecture and only encrypted management traffic is sent to the cloud. Customer data traffic is never sent to the cloud.



WatchGuard APs are cloud-managed, but provide full functionality even when Internet access is unavailable. For example, when a WatchGuard AP reboots without access to the Internet, the AP uses a locally stored configuration to operate.

Because WatchGuard APs operate without a controller, these features and functionality are performed at the AP level:

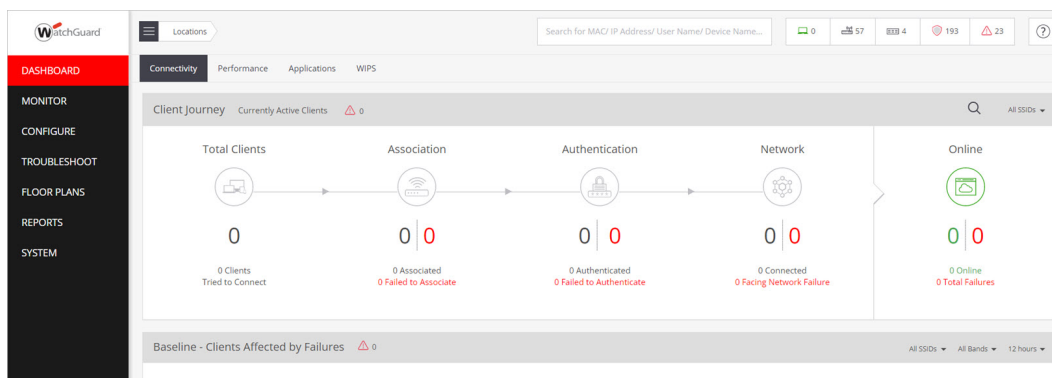
- QoS (Quality of service) and traffic shaping
- RF management
- Bonjour gateway
- Application visibility
- WIPS (Wireless Intrusion Prevention System)
- Compliance
- SSID scheduling

Cloud-based Management with WatchGuard Discover

WatchGuard Wi-Fi Cloud and WatchGuard APs eliminate the cost and complexity of traditional controller-based enterprise wireless network solutions, to simplify deployment. This makes it an ideal solution for organizations with a limited IT staff, distributed sites, and a tight IT budget.

The WatchGuard Discover interface is designed for cloud applications. The interface is lightweight and can be used on any Web browser, OS, or device, including Android devices, iPads, and other tablets. Dashboards and widgets optimize the information display according to their needs and screen sizes.

The unique hierarchical location-based policy management architecture simplifies management of multiple locations from a single UI. You can define role-based administration, Wi-Fi configurations, WIPS policies, and perform monitoring and troubleshooting in a logical context to specific locations.



Trusted Wireless Environment with WIPS

A Trusted Wireless Environment is a framework used to build a complete Wi-Fi network that is fast, easy to manage, and most importantly, secure. A Trusted Wireless Environment is based on these three core concepts:

1. **Market-Leading Performance:** You should never be forced to compromise security to achieve adequate performance to support your environment with the speed, connections and density that it requires.
2. **Scalable Management:** With easy set-up and management, you should be able control your entire wireless network, big or small, from a single interface and execute key processes to safeguard the environment and its users.
3. **Verified Comprehensive Security:** You should be able to prove that your security solution defends your business against Wi-Fi attacks and can deliver on the following benefits:
 - Provide automatic protection from the six known Wi-Fi threat categories:
 - Rogue access point
 - Rogue client
 - Neighbor access point
 - Ad-hoc connection
 - Evil Twin access point
 - Misconfigured access point
 - Allow legitimate external access points to operate in the same airspace
 - Prevent user connections to unsanctioned Wi-Fi access points

For more information, see [Trusted Wireless Environment](#) on the WatchGuard web site.

For detailed information on how to configure Wi-Fi Cloud WIPS to meet the requirements of a Trusted Wireless Environment, see [Create a Trusted Wireless Environment with WIPS](#).

You can test your own wireless network security measures to see if they are able to detect and prevent the six known threats identified by the Trusted Wireless Environment. For more information, see the [Trusted Wireless Environment Test Guide](#).

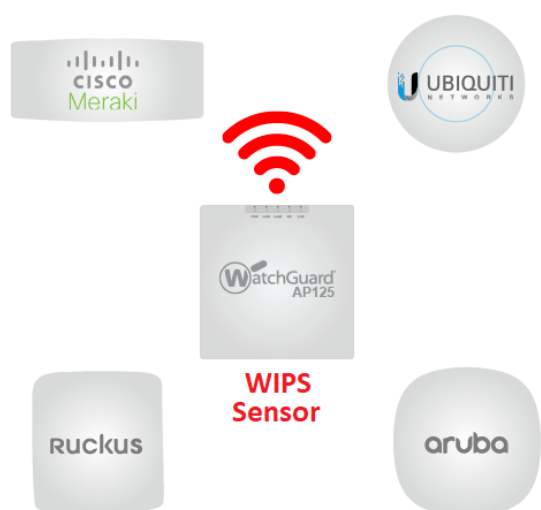
Create a Trusted Wireless Environment with WIPS

WIPS (Wireless Intrusion Prevention System) is a best-in-class wireless security architecture based on several patents. The system provides comprehensive protection from wireless threats, such as rogue APs, ad-hoc networks, client mis-associations, honeypots and evil twin APs, DoS attacks, and BYOD (Bring Your Own Device) risks including mobile hotspots.

With WIPS, it is easy to quickly create a Trusted Wireless Environment and automatically protect your Wi-Fi network against the six common Wi-Fi threat categories. WIPS is a collection of features that run on WatchGuard APs and Wi-Fi Cloud.

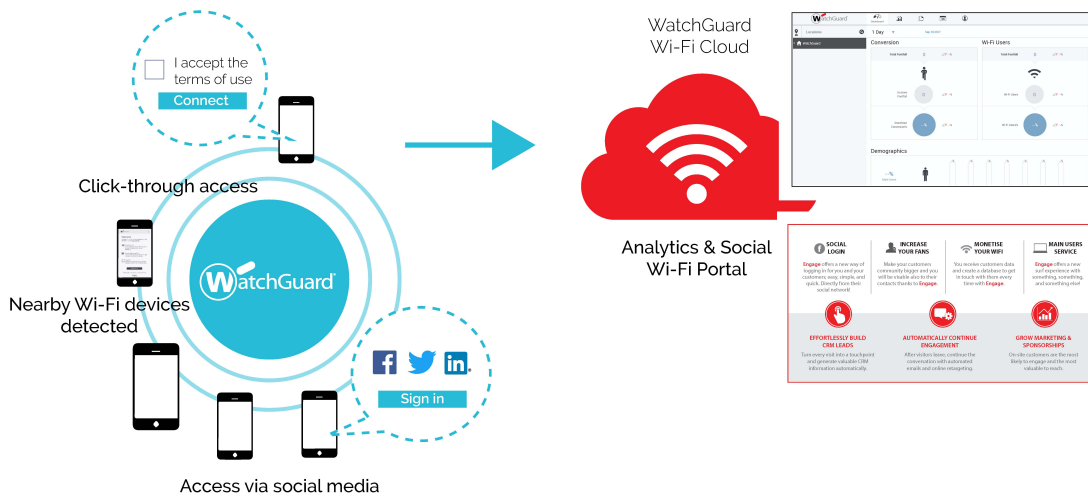


You can use WatchGuard APs for both Wi-Fi access and WIPS security protection, or you can use APs as dedicated WIPS security sensors that you can deploy alongside other WatchGuard APs or third-party APs and Wi-Fi controllers.



WatchGuard Analyze

WatchGuard Analyze provides enhanced guest management features to enable guest Wi-Fi access with social media, SMS, Guest Book, and Web Form plug-ins. Social media authentication gives guest Wi-Fi users the option to share their public profile information for social engagement.



Scalable, Multi-Tenant, Elastic Cloud Architecture

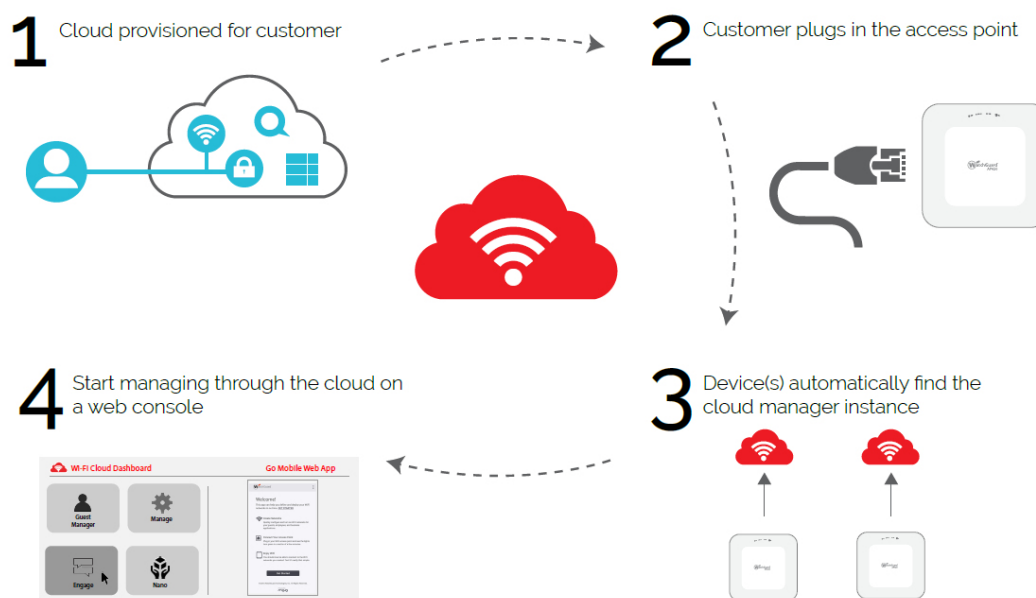
Powered by a mature, elastic cloud technology in development since 2008, Wi-Fi Cloud can scale to any number of locations. Built-in multi-tenancy enables account information, configurations and data to be completely segmented for different customers.

The data centers offer 99.9% up-time with local and WAN-based high availability and disaster recovery.

WatchGuard APs are managed from the cloud over a secure AES-encrypted tunnel. APs are capable of standalone operation and provide uninterrupted service with full functionality even if the AP loses connectivity to Wi-Fi Cloud.

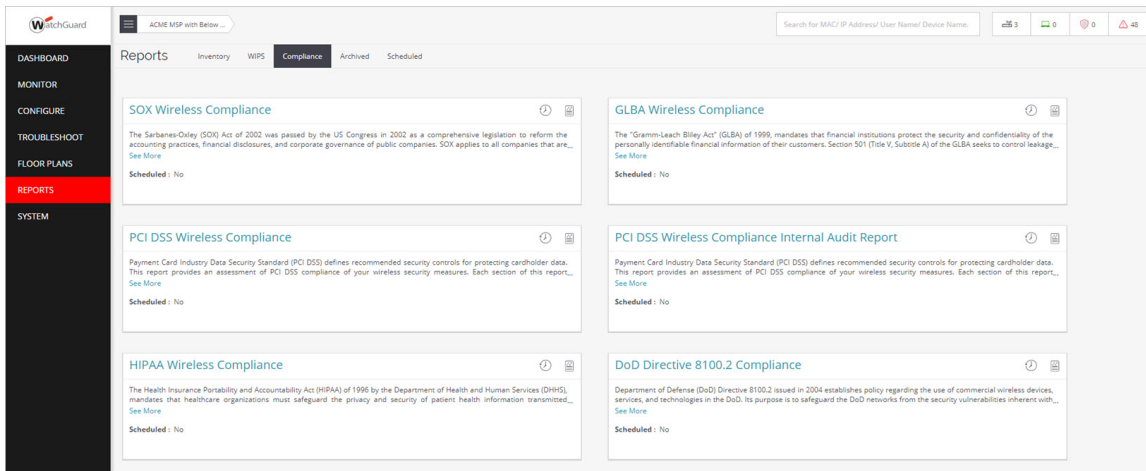
Zero Touch Deployment

WatchGuard APs can automatically discover and connect to W-Fi Cloud as soon as they are powered up and receive Internet access. This simplifies deployment, especially at remote sites without IT staff. When APs are configured in W-Fi Cloud for a location, the policies and configurations assigned to that location are automatically pushed to the device to immediately deploy the AP when it connects to the Internet.



Regulatory Compliance Reports

WatchGuard Wi-Fi Cloud enables organizations to meet wireless security requirements defined by their respective regulatory compliance standards. The audit process is simplified with predefined HIPAA and PCI compliance reports that map wireless vulnerabilities and threats to specific requirements. From WatchGuard Discover, you can generate reports across many locations. You can generate reports on-demand or schedule reports for automatic generation, and they can be archived or delivered by email.



Wireless Network Design

Before you deploy WatchGuard APs on your network, you must research, design, and plan your wireless network deployment to make sure it meets your requirements for coverage, capacity and airtime demand, and security.

Evaluate Requirements

When you evaluate your current environment and wireless requirements, make sure to consider:

- What wireless modes must your access point support (802.11a/b/g/n, 802.11ac Wave 1, Wave 2)?
 - What types of wireless clients do you want to allow to connect?
 - What wireless modes do they typically support?
- What SSIDs and networks do you want to create?
 - Are there groups of wireless users who need wireless access to different network resources?
 - Do you want to set up a guest wireless network that only allows Internet access?
- Where is the best physical location for each AP?
 - What is the physical size of the environments wireless users will connect from?
 - Do you need more than one AP to cover multiple areas?

Coverage Planning

Traditional coverage planning examines the physical environment where the wireless network will be deployed and the different factors that can affect your wireless signal power, range, and attenuation.

Coverage planning provides:

- Optimal frequency usage and access point locations
- Determination of transmit power levels
- Prevention of channel interference
- Examination of floor plans, physical obstructions, and building materials

Capacity Planning

As part of your wireless deployment planning you must also consider capacity and airtime demand. You must factor in to your plan the expected peak airtime demand amount and type of traffic, and traffic patterns for your wireless network and the coverage area it serves.

For example, a deployment for a hotel and its conference rooms has very different capacity and airtime demand criteria than a deployment for a small office, a retail department store, or a school campus. Each wireless deployment is unique and requires both coverage and capacity planning.

Capacity and airtime demand analysis provides:

- Optimal number of clients per access point radio, including idle and active clients. You must factor in slow periods and worst-case usage scenarios.
- Airtime demand and minimum data rates for different types of application traffic.
 - Include email, web, video, social media, streaming, and other applications.
 - Determine bandwidth throughput per application and connection, then determine aggregate bandwidth required in the wireless network coverage area.
- Considerations for growth, based on the number of connected clients and application bandwidth usage

Wireless Site Survey

Complete a wireless site survey to analyze your physical environment and existing wireless signals.

Use a wireless site survey utility, such as Ekahau HeatMapper, AirMagnet Planner, or any other similar tool.

- Measure before the deployment as part of your planning
 - Measure any existing wireless signals and interference in your environment
 - Measure wireless signal strength at different locations.
- Measure after the deployment to see the AP signal strength and range
 - After you install your access points, make another heat map to verify that your current placement provides adequate coverage and signal strength.
 - Check for wireless channel congestion and make sure the distance between APs does not degrade the signal to problematic levels

Channel Capacity Planning

Most wireless networks are designed for capacity rather than coverage, especially in educational environments where high client densities and high bit rate applications, such as video streaming, are common.

To design networks based on capacity, the first step is to define the requirements, which include client density, client types, applications, use cases, and throughput requirements.

For a successful design, you also need other information related to the environment. This includes factors such as Wi-Fi spectrum availability, building layouts, building materials used, and neighbor Wi-Fi channel usage.

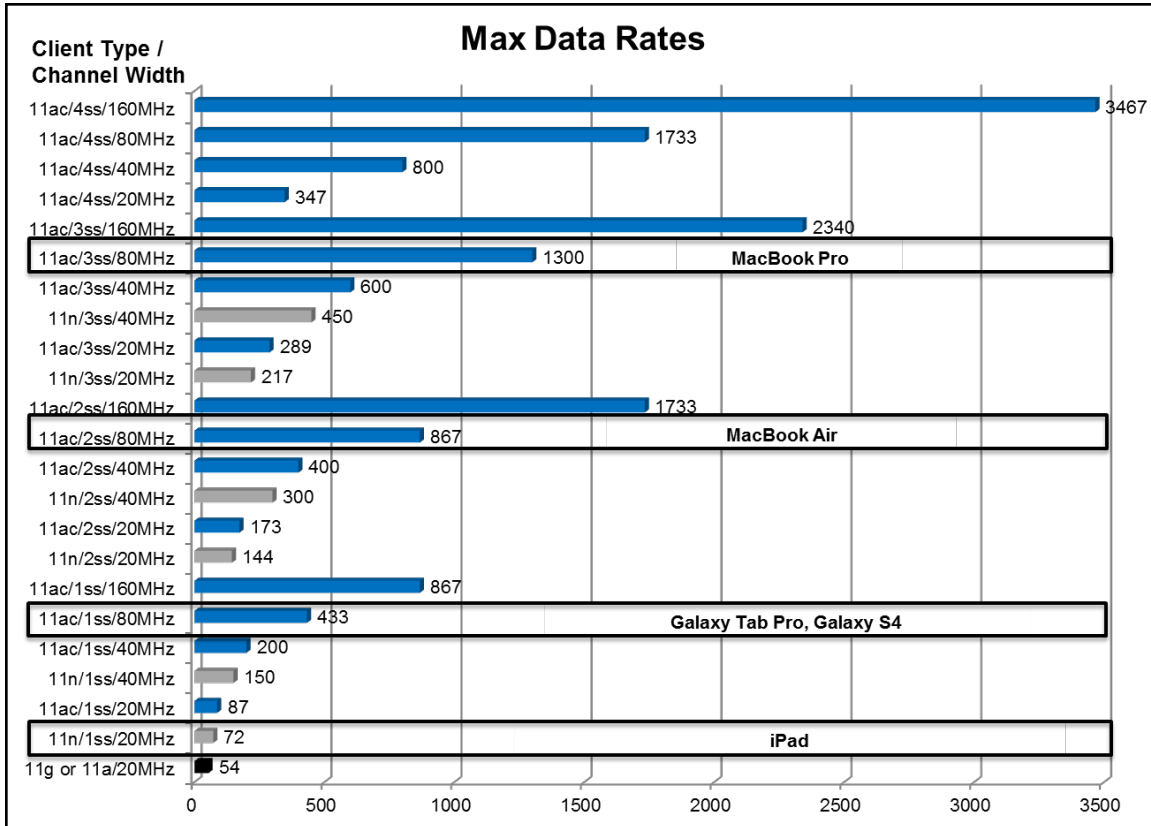
Design Wireless Networks for Capacity

The design process includes these analysis and planning stages:

- Requirements Analysis (Clients, Applications, Use Cases)
- Environment Analysis
- Channel Capacity Planning

Requirements Analysis – Clients

You must determine the number and types of client devices and where they are located on the network. Channel capacity and overall network capacity are as much a function of the client population as the types of APs and switches deployed. While it is not always possible to know the exact breakdown of client capabilities (for example, 802.11n vs. 802.11ac, Wave 1 or Wave 2 802.11ac, 1x1, 2x2, and 3x3) for a given area of the network, the more details that you know, the more accurate your channel capacity planning will be. Often you can use monitoring tools in the current Wi-Fi deployment to gather details about the clients in use on your network.



For example, when you compare the maximum data rate of the 1x1 Samsung Galaxy Tab Pro (433 Mbps) to that of the 3x3 Apple MacBook Pro (1.3 Gbps), you can see that the MacBook Pro has approximately three times the maximum data rate of the Galaxy Tab Pro. A wireless network that has only MacBook Pro clients could require as much as three times the capacity of a wireless network with only Galaxy Tab Pro clients.

Requirements Analysis – Applications

You must determine which applications are typically used on your wireless client devices. To estimate a per-client Mbps throughput requirement for a given area of a deployment, use the application with the highest bit rate. For example, in a classroom the highest bit rate application could be HD video streaming at 5 Mbps. For this use case, we recommend a per-client throughput requirement of 5 Mbps. To determine which applications are used by your wireless clients, you can use application visibility tools on your current wireless network.

It is also important to consider the requirements for applications that you plan to use in the future. We recommend you communicate with IT personnel about proposed future application use.

These are reference approximate bit rates for common applications. You can use these values to calculate approximate capacity requirements.

Application	Approximate Average Bit Rate
Audio	100-1 Mbps
File Backups	20-60 Mbps
File Sharing	5 Mbps
On-Line Testing	2-4 Mbps
Printing	1-3 Mbps
Video Conferencing: Standard Definition	5-1 Mbps
Video Conferencing: High Definition	2-3 Mbps
Video Gaming*	Requires measurements
Video Streaming: Standard Definition	1 Mbps
Video Streaming: High Definition 720p	3-5 Mbps
Video Streaming: High Definition 1080p	8-12 Mbps
Video Streaming: UHD (4K)	18-25 Mbps
Webinars	1 Mbps
Web Browsing	750 Kbps

** We recommend that you complete an over-the-air packet capture or use the Application Visibility feature in WatchGuard Wi-Fi Cloud to measure the application bit rate on your current wireless network.*

Use Cases

A use case is defined as the number and types of devices and their applications and usage patterns for a specific location. To learn about use cases for a deployment, we recommend you perform a thorough site walk-through with IT personnel familiar with the current network. You can also find solutions for several use cases for a school campus deployment in the [Deployment Use Cases](#) section.

Environment Analysis

Wireless Environmental Factors

There are several environmental factors that can affect the range and performance of wireless networks. You must estimate the path loss and attenuation of your wireless signals because of these factors.

Walls and ceilings

Walls and ceilings between the AP and wireless clients can degrade signal strength. Wireless signals can penetrate walls and other structures, but the rate of penetration is directly related to the type of building materials, material thickness, and the distance from the wireless antenna.

Building materials

Metal and aluminum doors, glass, concrete, metal studs, brick walls, glass, and other types of building materials can have a significantly negative effect on the strength of wireless signals.

EMI (Electro-magnetic interference)

EMI from other electrical devices, such as microwaves, cordless phones, and wireless headsets can generate significant RF noise and degrade or disrupt wireless communications.

Distance

Wireless signals degrade quickly past their maximum range. You must plan your network carefully to provide adequate wireless coverage over the range you require in your environment.

Wireless Regulatory Domain

The number of channels potentially available for a deployment depends on the regulatory domain where the deployment is located. Some regulatory domains have greater spectrum capacity than others. The amount of spectrum available for a given deployment has a direct impact on the types of uses cases you can support.

RF Environment

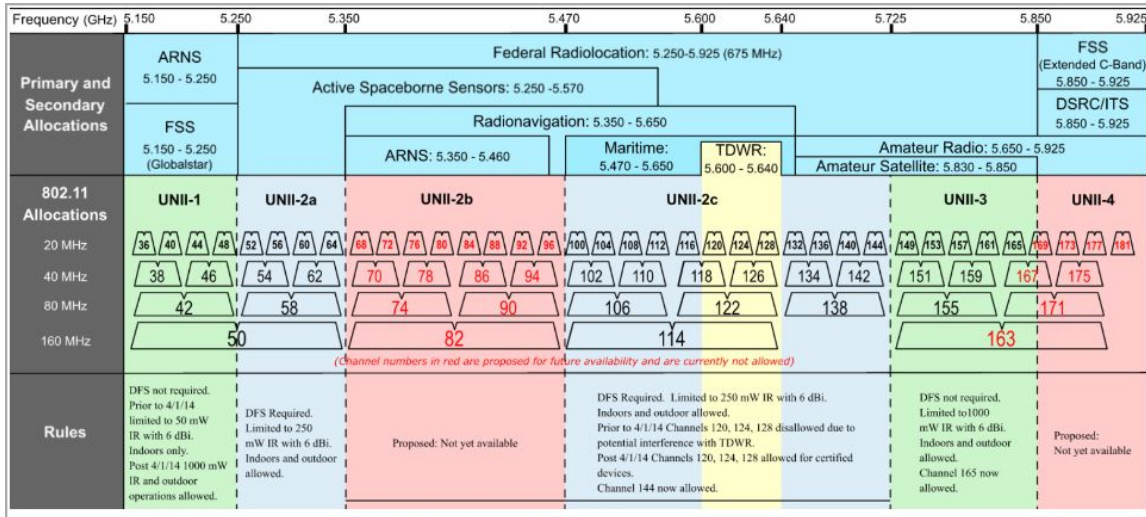
You must assess the RF (radio frequency) environment to identify local sources of Wi-Fi and non-WiFi interference. For example, RF environments for schools located in dense urban areas have a higher potential interference than for schools located in rural areas.

Channel Capacity Planning

As part of capacity planning you must review and understand the wireless spectrum availability to help guide the planning process.

Spectrum Availability in 5 GHz

This diagram describes the current and proposed spectrum for the regulatory regions covered by the FCC (Federal Communications Committee) in the United States.



FCC 5 GHz Frequency Allocation. Source: wlanpros.com

All spectrum is currently available in FCC regions except for the frequencies displayed in pink. These frequencies are not currently available, but may be available to the Wi-Fi spectrum in the future. Even if you use all channels currently available, including DFS (Dynamic Frequency Selection) channels, it can be a challenge to meet the capacity requirements of some high density and high throughput use cases.

This table shows the number of channels available for the 5 GHz band in the US.

Channel Width	Without DFS	With DFS
20 MHz	9	25
40 MHz	4	12
80 MHz	2	6
160 or 80+80 MHz	1	3

Most networks deploy 40 MHz or 80 MHz channels based on use case requirements and spectrum availability. Some notable exceptions are high density auditorium or stadium and arena deployments where it is often preferable to use 20 MHz channels because of the ability to reuse channels. We recommend you consider the use of 80 MHz channel plans only if DFS channels are available, because without DFS channels only two non-overlapping 80 MHz channels are available. If you use DFS channels, you have six non-overlapping DFS channels available.

802.11ac Wave 1 and Wave 2

This table provides a high-level comparison between the 802.11ac Wave 1 and Wave 2 standards.

Feature	Wave 1	Wave 2
Channel Width	20, 40, 80	20, 40, 80, 80+80, 160 MHz
QAM Encoding	16, 64, 256 QAM	16, 64, 256 QAM
Spatial Streams	3	4 (as implemented) Up to 8 (per the standard)
Explicit Beamforming	Some Wave 1 APs	All Wave 2 APs
MIMO	SU-MIMO	SU-MIMO, MU-MIMO
Frame Aggregation	A-MSDU size 11,426 Bytes A-MPDU size 1,048,576 Bytes	A-MSDU size 11,426 Bytes A-MPDU size 1,048,576 Bytes
Bands Supported	5 GHz	5 GHz
Forward Error Correction	BCC (Binary Convolutional Code) LDPC (Low Density Parity Check)	BCC (Binary Convolutional Code) LDPC (Low Density Parity Check)
Dynamic Channel Width	Some Wave 1 APs	Most Wave 2 APs

MU-MIMO

MU-MIMO (Multi-User MIMO) can improve performance in several use cases because of its ability to enable simultaneous transmissions from APs to clients. In regular 802.11 communications, AP-to-client transmissions are serial communications. With MU-MIMO, up to four AP-to-client transmissions can occur simultaneously, which can significantly improve performance and capacity in many use cases.

The boost in performance and capacity depends on several factors, such as channel conditions, client density, client capability, and client mix (SU-MIMO to MU-MIMO ratio). Early MU-MIMO performance testing has shown that when conditions are optimal, aggregate throughput performance can improve by as much as 50%.

The MU-MIMO solution may be able to support HD video, while the Wave 1 solution may only be able to support standard definition video.

MU-MIMO helps in deployments with high-density areas such as auditoriums and classrooms where aggregate throughput demands can be high. Both of these use cases primarily support 1x1 and 2x2 clients. These types of clients are well suited to take advantage of MU-MIMO. Both APs and clients must support Wave 2 to realize the benefits of MU-MIMO.

The WatchGuard AP420 is a high-powered 802.11ac Wave 2 access point, and supports up to four spatial streams in both SU-MIMO and MU-MIMO modes. Earlier generations of Wave 2 APs support up to three spatial streams in MU-MIMO mode. The additional spatial stream for MU-MIMO with the AP420 helps improve wireless network performance and capacity. The AP420 simultaneously supports up to 64 MU-MIMO clients that are dynamically combined for optimal MU-MIMO transmissions of up to 4 MU-MIMO clients at a time.

The AP420 is the recommended platform for most large environments, such as classrooms, cafeterias, auditoriums, libraries, and lecture halls.

DFS Channels

In the past, wireless network designers were reluctant to deploy DFS channels because of concerns about lack of client support and network instability caused by radar event detection. However, many networks today rely on DFS channels to meet higher scalability requirements. Because radar events are not as common as once thought (for most deployments), and newer Wi-Fi devices support DFS channels, DFS-enabled wireless networks are now more common.

We recommend you enable DFS channels if they are available, and that you provision both 5 GHz and 2.4 GHz bands. You can also enable 2.4 GHz coverage throughout the deployment as a best practice to provide access for clients that use both bands.

Channel Width Selection

Wider channel widths such as 80 MHz and 160 MHz provide greater bandwidth and data rates compared to smaller channel widths (20 and 40 MHz), but this also means fewer channels are available and increases the possibility of co-channel interference in dense environments.

For example:

- 160 MHz – Only two channels are available
- 80 MHz – Provides 6 non-overlapping channels if DFS channels available
- 40 MHz – Provides 12 non-overlapping channels if DFS channels available
- 20 MHz – Many channels and combinations available

Channel width selection depends on several factors including use case requirements, spectrum availability, RF environment, and budget for the number of APs required. In a deployment in which you cannot use DFS channels (and must therefore use 40 MHz channels), you might need to reconsider your requirements. For example, you might need to decrease the bit rate at which video is streamed for 2.4GHz-only clients and for dual band clients that do not support DFS channels. Deploy 2.4 GHz throughout your network to provide some additional capacity.

In general, these channel widths are recommended:

- High density and non-DFS deployments – Use 20 or 40 MHz channels
- Low density and DFS channels available – Use 40 MHz channels
- Well-designed deployment with DFS channels available – 80 MHz channels

Estimate Channel Capacity

Capacity planning must be use-case specific and must consider these factors:

- Total active devices
- Types of devices
- Usage patterns
- Applications in use
- Area of coverage

Estimated throughput capacities for different channel widths and spatial streams are provided in this table, which you can use as a point of reference.

Maximum Data Rates				
	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	87 Mbps	200 Mbps	433 Mbps	867 Mbps
2 Spatial Streams	173 Mbps	400 Mbps	867 Mbps	1.73 Gbps

Maximum Data Rates				
3 Spatial Streams	289 Mbps	600 Mbps	1.33 Gbps	2.34 Gbps
4 Spatial Streams	347 Mbps	800 Mbps	1.73 Gbps	3.47 Gbps

These rates are maximum data rates and not throughput capacity rates. Throughput capacity rates are much lower because of factors such as protocol overhead, contention loss, and loss due to signal strength degradation.

See [Channel Capacity Estimates](#) for a series of tables that estimate channel capacities for different rates of contention loss and loss caused by signal strength degradation for different channel widths and spatial streams. You can reference these tables to simplify the channel capacity planning process.

Channel Capacity Estimate Considerations

The channel throughput capacity estimates provided here and in [Channel Capacity Estimates](#) are derived from single AP and multi-AP competitive performance testing. The estimations factor in contention loss seen in tests for 5, 10, 20, 30, 40, 50 and 60 clients per radio where all clients are located within 20 feet (6.096 meters) of the AP under test.

To estimate loss caused by rate adaptation because of lower signal strength, clients are placed from 10 to 60 feet (3.048 - 15.24 meters) away from an AP.

While capacity loss from wireless interference such as co-channel interference (CCI) and adjacent channel interference (ACI) can be substantial, it is not factored into this test data.

This table shows the maximum throughput rates for different channel widths and spatial streams estimated to be 60% of the maximum data rate. This is a conservative number. For example, in certain circumstances, a three spatial stream client (for example, a MacBook Pro) connected to a three spatial stream AP configured for 80 MHz can achieve total throughput of 850 Mbps, which is higher than the listed value of 798 Mbps.

Estimated Max Throughput Capacity - 60 % Max Data Rate				
Client Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	52 Mbps	120 Mbps	260 Mbps	520 Mbps
2 Spatial Streams	104 Mbps	240 Mbps	520 Mbps	1.04 Gbps
3 Spatial Streams	173 Mbps	360 Mbps	798 Mbps	1.40 Gbps
4 Spatial Streams	208 Mbps	480 Mbps	1.04 Gbps	2.08 Gbps

Actual use cases are unlikely to have a single client active so the table above is useful only as a benchmark to measure AP performance. When you factor in higher client densities common to large deployments, throughput capacity of a radio declines. You can reference the tables in [Channel Capacity Estimates](#) for planning examples, as well as for the use cases presented later in this guide.

Channel Capacity Calculations

This section provides a method to manually calculate channel capacity.

To calculate channel capacity, you must:

- Determine the percentage of airtime or channel utilization that an individual client requires to meet a per client throughput requirements for a particular use case.
- Determine the total channel capacity needed to accommodate all clients in the use case.

For example, a use case has 150 MacBook Pros (or other 11ac 3x3 clients) active concurrently. Each client has a throughput requirement of 2 Mbps. DFS channels are not available so we must use a 40 MHz channel plan.

Before you start your calculations, you must know the estimated channel capacity per radio and an estimated density per radio. This information is required to find the estimated channel capacity in [Channel Capacity Estimates](#). This use case will likely fall into the very high client density category as there will be 150 concurrently active clients.

Use Case	Device Type	Number of Active Devices/Density	App or Throughput Requirement Bit Rate	Channel Capacity	Per Device Airtime / Channel Capacity
Library	MacBook Pro/3ss	150 / Very High	2 Mbps	120 Mbps / 40 MHz	1.67%

The very high client density table in [Channel Capacity Estimates](#) shows that for 11ac 3x3 client with a 40 MHz channel, the estimated throughput capacity is 120 Mbps. To determine the percentage of airtime or channel utilization an individual client requires to meet a per-client throughput requirement, divide the throughput requirement by the estimated channel capacity and multiply by 100.

- $(\text{Application Bit rate or Throughput Requirement}) / (\text{Channel Capacity}) \times 100 = \text{Per Device Airtime}$
- $(2 \text{ Mbps} / 120 \text{ Mbps}) \times 100 = 1.67\%$
- Per Device Airtime = 1.67%

You can use this number to calculate the total number of channels/radios required to meet the use case requirements.

Use Case	Device Type	Number of Active Devices / Density	Per Device Airtime	Total Airtime	Estimated Channels / Radios Required
Library	MacBook Pro/3ss	150/Very High	1.67%	250%	3

You must multiply the per-client airtime required and the total number of clients active concurrently.

- Number of Active Devices x per Device Airtime = Channels/Radios Required
- 150 Active Devices x 1.67% per Device Airtime = 250%
- Estimated Channels/Radios Required = 3 (Rounding up)

Maximum Clients For APs

This table lists the recommended maximum number of associated and active clients for currently available WatchGuard APs.

Model	Description	Recommended Use	Maximum Associated Clients	Recommended Concurrent Active Clients
AP120 (Legacy)	Dual radio, 802.11ac Wave 1, 2x2, Indoor	Low density / throughput areas	254	50
AP320 (Legacy)	Dual radio, 802.11ac Wave 1, 3x3, Indoor	Medium density / throughput areas	254	75
AP322 (Legacy)	Dual radio, 802.11ac Wave 1, 3x3, Outdoor	Outdoors	254	75
AP125	Dual radio, 802.11ac Wave 2, 2x2, Indoor	Low density / throughput areas	254	50
AP225W	Tri radio, 802.11ac Wave 2, 2x2, Indoor, Wall Plate	Low to medium density / throughput areas	254	75
AP327X	Dual radio, 802.11ac Wave 2, 2x2, Outdoor	Outdoors	254	75
AP325	Tri radio, 802.11ac Wave 2, 2x2, Indoor	Low to medium density / throughput areas	254	75
AP420	Tri radio, 802.11ac Wave 2, 4x4, Indoor	High density / throughput areas	510	150

Summary of Channel Capacity Planning Recommendations

This table summarizes the channel capacity planning recommendations for wireless networks.

Recommendations	Notes
Design wireless network for capacity.	
Focus design on specific use cases.	Use Case = Number of devices + types of devices + set of applications + usage patterns + for a given area.
Use most demanding application (per use case) to determine throughput requirement.	If application information is unknown, design for a per client throughput requirement of 5 Mbps.
Use current wireless network to determine type and number of devices per use case.	
Use current wireless network tools to determine application bit rates.	Alternatively, packet capture tools can be used to determine application bit rates.
Select the correct APs for the use cases.	Refer to the recommended maximum clients per AP table for AP selection.
Use predictive planning tools to estimate the number of APs required to meet use case throughput requirements.	
Design for 5 GHz capacity.	Deploy both 2.4 GHz and 5 GHz pervasively.
Use DFS channels.	Discover if any DFS channels cause interference with local radar and remove those channels from the potential operating channel pool.
Use 20 or 40 MHz channels.	If several DFS channels cannot be used, then plan to use 40 MHz channels.

Site Preparation Checklist

For a successful deployment, you must prepare the installation site. This section provides a checklist to help the implementation team with site preparation.

Preparation Checklist	Notes
Installation Preparation	
Site survey	<p>WatchGuard recommends you ideally perform an on-site survey of AP / wireless client performance checks with the clients that are representative of the devices used at the location (Smart phones, tablets, laptops, etc.)</p> <p>Alternately, if an on-site survey is not feasible, use a predictive site survey based on the documented details of all aspects of the deployment, including network architecture, clients, applications, physical environment, floor plans etc.)</p> <p>WatchGuard provides to partners a <i>Wi-Fi Customer Requirements Questionnaire</i> to assist in creating predictive site surveys. For more information, log in to your partner account on the WatchGuard web site and go to Product > Selling Secure Wi-Fi.</p>
Client survey	Determine the proportion of wireless devices per user and their function.
POE or AC power	See the "AP Power Requirements" section in Wired Network Best Practices .
Cable plant (CAT5e or greater)	See the Cable Category Reference table.
Ladder/Scissor Lift	
Special AP mounting requirements	AP mounting instructions are available in the WatchGuard AP Hardware Guides .
Internet availability	
Tools for mounting APs	
Implementation Preparation	
Network switch ports	
DHCP	

Preparation Checklist	Notes
RADIUS	
DNS IPs	
VLAN IDs	
Firewall rules: <ul style="list-style-type: none"> ■ Port 3851 (UDP) outbound ■ Port 3852 (UDP) outbound for APs configured in CIP mode ■ Port 80 (TCP) outbound / stateful inbound ■ Port 443 (TCP) outbound / stateful inbound 	These are the required ports for WatchGuard APs to communicate with WatchGuard Wi-Fi Cloud at these domains: *.cloudwifi.com redirector.online.spectraguard.net
Proxy bypass rule for AP management traffic	Bypass rule is for management traffic from the AP's IP address to WatchGuard Wi-Fi Cloud.
Verification Preparation	
Wi-Fi clients	Clients are required for acceptance testing. Make sure the clients are representative of the devices used at the location.
Acceptance test plan	The acceptance test plan should verify client and application functionality for all applications used at the site.

Getting Started with WatchGuard Wi-Fi Cloud

A Wi-Fi Cloud AP deployment includes these configuration steps:

- Activate APs
- Connect the APs to WatchGuard Wi-Fi Cloud
- Create a Wi-Fi network SSID
- Configure AP device and radio settings

For details on how to perform a basic set up of your APs in Wi-Fi Cloud, see the [WatchGuard Wi-Fi Cloud Getting Started Guide](#).

Getting Started with WIPS

A WIPS security configuration includes these features:

- Auto-classification settings for APs and clients
- Authorized WiFi Policies
- Automatic Intrusion Prevention settings

For detailed information on how to configure Wi-Fi Cloud WIPS to meet the requirements of a Trusted Wireless Environment, see [Create a Trusted Wireless Environment with WIPS](#).

Deployment Best Practices

This section describes deployment best practices for these network factors:

- [*Wireless Network Best Practices*](#)
- [*Wired Network Best Practices*](#)
- [*Network Services Best Practices*](#)
- [*AP Placement and Channel Plan Best Practices*](#)

These recommendations are based on successful wireless deployments. Because each wireless deployment has its own unique environment, client use cases, and network architecture, these best practices are intended as guidelines.

Wireless Network Best Practices

This section provides suggestions on how to deploy a wireless network that can support large high-density use cases. The recommended settings are based on the features available in WatchGuard Wi-Fi Cloud.

AP Transmit Power Reduction

When you reduce AP transmit power, it helps to decrease the cell size. Smaller cells enable network designs to maximize channel reuse that can increase aggregate throughput and capacity for a wireless network.

Classroom:

- 5 GHz: 8-16 dBm
- 2.4 GHz: 4-10 dBm

Auditorium or Lecture Hall:

- 5 GHz: 5-12 dBm
- 2.4 GHz: 3-10 dBm

We recommend that you set AP transmit power levels for 2.4 GHz lower than those for 5 GHz. This is to compensate for better propagation of 2.4 GHz signals as compared to 5 GHz.

To configure the Transmit Power:

1. Open Discover.
2. Select **Configure > WiFi > Radio Settings**.
3. Expand the **Radio Advanced Settings** section.
4. Configure the Transmit Power for the radio, or select **Automatic** to automatically adjust power settings based on the RF environment.

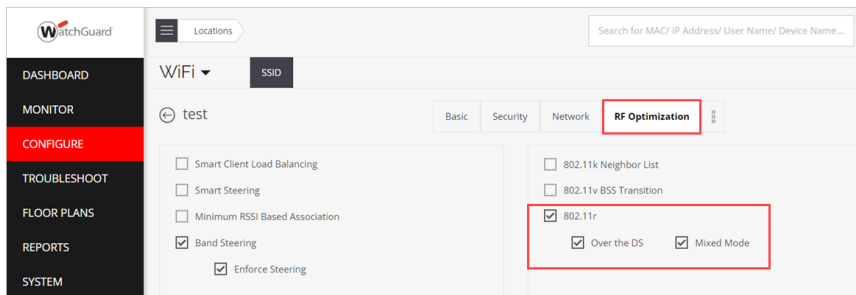
The screenshot shows the 'Advanced Radio Settings' section of the WatchGuard Wi-Fi Cloud configuration interface. It features a 'Transmit Power Selection' section with two radio buttons: 'Auto' (selected) and 'Manual'. Below this, there are four input fields with dropdown menus: 'Loudness RSSI' (set to -75 dBm [-95 to -45]), 'Neighbor Count' (set to 3 [1-10]), 'Minimum Transmit Power' (set to 4 dBm [4 - 30]), and 'Maximum Transmit Power' (set to 30 dBm [4 - 30]). At the bottom, there is a checkbox labeled 'Use External Antennas' which is currently unchecked.

Fast Roaming

WatchGuard APs support 802.11r fast roaming. The 802.11r standard significantly improves roaming times and can significantly improve streaming quality while roaming. The 802.11r feature is enabled per SSID. We recommend you enable 802.11r with mixed-mode support so that SSIDs support both 802.11r and non-802.11r clients.

To configure 802.11r fast roaming settings

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **RF Optimization** tab.
5. Select the **802.11r** check box.
6. Select the **Over the DS** and **Mixed Mode** settings as required.
7. Save the SSID settings.



802.11k and 802.11v

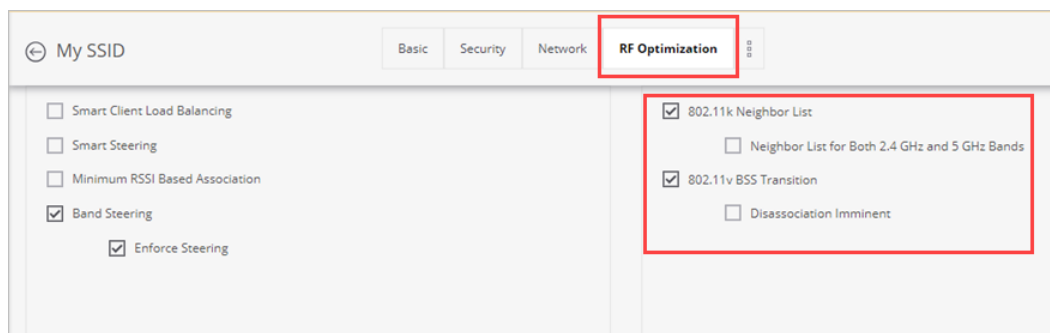
The wireless network infrastructure can influence client roaming decisions with features such as load balancing, however, the final roaming decision is decided by client devices. The IEEE amendments 802.11k and 802.11v define enhanced information exchange that enables clients to make more informed roaming decisions.

Radio Resource Measurement (802.11k) and Wireless Network Management (802.11v) help measure, report and manage resources on a wireless network. With 802.11k, APs and clients share RF environment information. With 802.11k enabled, clients can make more informed roaming decisions with respect to the RF environment, such as channel load, link measurement, noise histogram, and neighbor reports. With 802.11v enabled, some RF information is exchanged, such as channel usage, but many other types of information are also shared, such as BSS transition management, Flexible Multicast Service (FMS), QoS traffic capability, and location services capabilities.

We recommend you enable both 802.11k and 802.11v, and with backwards compatibility mode enabled, so that devices that do not yet support these newer specifications can still join the wireless network.

To configure 801.11k and 802.11v options:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **RF Optimization** tab.
5. Select the **11k Neighbour List** and **11v BSS Transition** check boxes.
6. Save the SSID settings.



SSID Bridge vs. NAT Mode

WatchGuard APs can operate in Bridged mode, NAT (Network Address Translation) mode, or Tunneled mode.

For most use cases other than small remote sites we recommend you use bridged mode. With bridged mode, traffic is bridged between the wireless interface and the wired interface. When you use NAT mode, the AP supplies clients with IP addresses from the built-in DHCP service on the access point and performs NAT for traffic between the wireless interface and the wired interface.

Tunneled mode is useful when you want to route network traffic on the SSID to and from a single end point, and apply policies at this end point. In the tunneled mode, APs on the SSID route all traffic via the tunnel to a remote endpoint configured on the Tunnel Interface that you select.

To configure bridge or NAT mode:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Network** tab.
5. Select **NAT** or **Bridged** mode.
6. Configure the options for the selected mode as required.
7. Save the SSID settings.

The screenshot shows the 'My SSID' configuration page in the WatchGuard Cloud AP interface. The 'Network' tab is selected and highlighted with a red box. Below the tab, the 'VLAN ID' is set to 0. The 'Bridged' mode is selected with a radio button, also highlighted with a red box. Other options include 'NAT' and 'Tunneled' modes, 'Layer 2 Traffic Inspection and Filtering', 'Inter AP Coordination' (with 'RF Neighbors' selected), 'Advertize Client Associations on SSID VLAN' (checked), and 'DHCP Option 82'.

Smart Client Load Balancing and Steering

In high-density environments, such as auditoriums, lecture halls, and libraries, APs are usually deployed close to each other to support a large number of devices in a small space. Because they are close in proximity, a client device at any given location can often detect multiple APs with good signal strength. Unless the client and the AP both support 802.11k (very few clients support 802.11k), the client typically picks the AP that it detects with the strongest signal strength. This can cause some APs in the network to be over-used while the other APs have capacity to spare. You can use Smart Load Balancing to distribute the clients across APs and across bands within an AP. This can increase per-client throughput, improve application performance, and increase the overall capacity of the wireless network.

Load balancing is also useful in moderately dense environments common to classrooms where clients require high bandwidth to support applications such as HD video streaming.

Smart Steering

Clients that prefer to remain connected to distant APs rather than roam to closer APs are a common wireless network issue. These clients not only experience poor performance, but because they operate at low data rates, they lower the capacity of the AP.

Smart Steering is a client-to-AP association optimization that enables the wireless network infrastructure to control client connectivity and roaming. Smart Steering monitors clients and automatically steers them to the optimal AP. This improves the performance for the steered client, and improves the performance for the AP from which the client disconnects. Smart Steering works with all types of clients and client operating systems.

You can configure advanced Smart Steering options in the **Radio Advanced Settings** section for an AP's radio settings. We recommend you use the default settings.

Band Steering

While most devices tend to associate to 5 GHz radios, there are some clients that must be directed towards the 5 GHz band. Band steering enables you to steer clients towards the 5 GHz band, and distributes the clients across both bands so that the channel capacity in the 2.4 GHz band can be used.

Advanced parameters are configured in the **Radio Advanced Settings** section for an AP's radio settings. We recommend you use the default settings.

You can enable load balancing and steering options in the **RF Optimization** settings of an SSID Profile.

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **RF Optimization** tab.
5. Select the **Smart Client Load Balancing** check box and other steering options as required.
6. Save the SSID settings.

My SSID

Basic Security Network **RF Optimization**

☒ Smart Client Load Balancing

☒ Smart Steering

☒ Minimum RSSI Based Association

☒ Band Steering

☒ Enforce Steering

☒ 802.11k Neighbor List

☐ Neighbor List for Both 2.4 GHz and 5 GHz Bands

☒ 802.11v BSS Transition

☐ Disassociation Imminent

Broadcast/Multicast Control

A large VLAN creates a large broadcast domain. Unnecessary broadcast and multicast traffic can consume valuable airtime. To prevent this, we recommend you configure broadcast/multicast control. You can block broadcast/multicast packets on your wireless network and create exemptions for specific applications.

To configure Broadcast/Multicast Control:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **RF Optimization** tab.
5. Select the **Broadcast/Multicast control** check box.
6. (Optional) Enable **Block Wireless to Wired** to block broadcast and multicast traffic from the wireless side to the wired side.
7. (Optional) Enable **Allow Bonjour** to allow the Apple Bonjour protocol. In many educational environments, multicast-based services such as Apple Bonjour are common. To enable Bonjour service advertisements, which use non-routable multicast addresses, to be transmitted across VLANs, a Bonjour gateway is required. WatchGuard APs have built in Bonjour Gateways that enable access to Bonjour services, such as Apple TVs and printers, across VLANs.
8. Configure the **Exemption list** for specific applications if required.
9. Save the SSID settings.

The screenshot shows the 'My SSID' configuration page with the 'RF Optimization' tab selected. A red box highlights the 'Broadcast/Multicast Control' section, which includes three checked options: 'Broadcast/Multicast Control', 'Block Wireless to Wired', and 'Allow Bonjour'. Below this is the 'Exemption List' section, which contains a table with columns for Name, EtherType, Destination MAC, Protocol, and Port. The Port column has a dropdown menu showing '[0-65535]'. An 'ADD' button is located at the bottom right of the Exemption List section.

Name	EtherType	Destination MAC	Protocol	Port
				[0-65535]

ADD

Alternatively, you can restrict VLAN sizes. WatchGuard Wi-Fi Cloud's controller-less architecture does not require tunneling all traffic back to a wireless controller located in the core of the network. This enables you to bring the VLANs out to the access switches. With VLANs at the edge of the network, the size of each VLAN can be controlled per building or per floor. VLAN size limiting helps you control broadcast and multicast bandwidth consumption.

Reliable Multicast Delivery and IGMP Snooping

Streaming multicast video over wireless is inherently challenging, as multicast traffic over wireless is not acknowledged by the receiving client. With no acknowledgments for multicast packets, multicast over wireless is essentially unreliable. Unicast packets must be acknowledged by the receiving client. If unicast packets are not acknowledged by the receiver, the sender resends the original packet.

For reliable delivery of multicast video, WatchGuard APs can convert multicast video traffic to unicast traffic at the 802.11 layer. Traffic is sent to the multicast address at the IP layer. If these unicast packets are not acknowledged by the receiver (for example, a client that has joined the multicast group) the AP resends the packet. This feature enables unicast traffic to be more reliable than multicast traffic. In addition to the reliable delivery feature of unicast packets, there is the additional benefit of the packets being sent at unicast data rates, which are typically much higher than multicast data rates, even when multicast rate optimization is enabled.

Multicast to unicast conversion is only part of the solution. You must enable IGMP snooping for optimal multicast video delivery. IGMP (Internet Group Management Protocol) enables WatchGuard APs to listen for multicast group join messages sent by wireless clients. The IGMP feature builds multicast group forwarding tables on the APs so that multicast traffic (now converted to unicast traffic) is transmitted to only those clients that have joined multicast groups.

To enable IGMP Snooping and create exceptions for specific IP addresses:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **RF Optimization** tab.
5. Select the **IGMP Snooping** check box.
6. (Optional) Add IP addresses to the **IGMP Snooping Exception list**. The packets with multicast IP addresses that are mentioned in the exception list are not dropped even if no client joins the multicast group. They are not converted to Unicast even if **Convert Multicast to Unicast** is enabled.
7. Save the SSID settings.

My SSID

Basic Security Network **RF Optimization**

☐ Broadcast/Multicast Control

☒ IGMP Snooping

IGMP Snooping Exception List

Enter IP Address

Snoop Timeout * 5 minutes [1 - 480]

You can specify up to 30 multicast IP addresses (range: 224.0.0.0 - 239.255.255.255)

☐ Convert Multicast to Unicast

Set a Minimum Unicast Rate

The default minimum unicast rate for 802.11n 2.4 GHz and 802.11ac 5 GHz is most suitable for networks designed to optimize coverage, as opposed to client capacity. We recommend that you design enterprise wireless networks for capacity with the goal to improve the throughput and client capacity of each cell and reduce cell sizes so that channels can be reused more frequently. This results in an increase in the overall capacity of the network, given a fixed amount of frequency spectrum to use.

One technique that can help reduce cell size is to increase the minimum data rate at which clients can associate to a wireless network. We recommend that you set the minimum unicast data rate to 24 Mbps.

To configure the minimum unicast data rate:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Traffic Shaping & QoS** tab.
5. Edit the minimum unicast data rate.
6. Save the SSID settings.

Unicast Rate Control

☐ Limit the maximum unicast traffic data rate to

0 Mbps [0 - 54]

☒ Limit the minimum unicast traffic data rate to

24 Mbps [0 - 54]

☐ Apply to all clients including 802.11n and 802.11ac

Multicast, Broadcast and Management Rate Optimization

This optimization feature enables you to configure the rate at which broadcast, multicast, and management packets are transmitted by the AP. You can increase the data rate for multicast, broadcast, and management traffic to improve wireless network performance. This feature can reduce the channel utilization consumed by these types of packets. This feature can also help reduce the effective network cell that enables greater channel reuse.

In addition to configuring management rate optimization, you can also restrict the number of SSIDs to significantly reduce the total airtime consumed by management traffic.

To configure the unicast and multicast data rates:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Traffic Shaping & QoS** tab.
5. In this example, the minimum unicast data rate has been set to 24 Mbps. Configure the data rate for multicast, broadcast, and management traffic to be equal to or greater than the minimum unicast data rate.
6. Save the SSID settings.

The screenshot shows a configuration window titled "Multicast, Broadcast and Management Rate Control". It contains two main sections: "Multicast, Broadcast and Management Rate Control" and "Unicast Rate Control".

In the "Multicast, Broadcast and Management Rate Control" section, there is a checkbox labeled "Set the data rate for multicast, broadcast and management traffic to" which is checked. Below this checkbox is a spinner control set to "24" and a text label "Mbps [0 - 54]". This entire section is highlighted with a red rectangular box.

The "Unicast Rate Control" section contains two checkboxes. The first, "Limit the maximum unicast traffic data rate to", is unchecked, with a spinner control set to "0" and a text label "Mbps [0 - 54]". The second, "Limit the minimum unicast traffic data rate to", is checked, with a spinner control set to "24" and a text label "Mbps [0 - 54]". At the bottom of this section, there is an unchecked checkbox labeled "Apply to all clients including 802.11n and 802.11ac".

Traffic Shaping

Most wireless networks offer guest access to clients. The Guest SSID may be available in limited areas of the deployment or it may be available across the entire network. If you offer guest wireless access, you must prevent guest traffic from adversely affecting your internal wireless network. To prevent guest users from disrupting wireless performance for non-guest users, you can configure rate limiting at the SSID level and client level .

To configure rate limits:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Traffic Shaping & QoS** tab.
5. Select the **Limit the maximum upload bandwidth on the SSID to** and the **Limit the maximum download bandwidth on the SSID to** check boxes.
6. Type a data rate from 0 to 1024 Kbps or Mbps.
7. Save the SSID settings.

The screenshot shows the 'My SSID' configuration interface. At the top, there are tabs for 'Basic', 'Security', 'Network', 'RF Optimization', and 'Traffic Shaping & QoS'. The 'Traffic Shaping & QoS' tab is selected and highlighted with a red box. Below the tabs, there is a section titled 'Number of Associations' with a checkbox 'Limit the maximum number of simultaneous associations to' and a value of 127. Below this, there is a section titled 'SSID Bandwidth Control' which is also highlighted with a red box. It contains two checked options: 'Limit the maximum upload bandwidth on the SSID to' and 'Limit the maximum download bandwidth on the SSID to'. The upload bandwidth is set to 10 Mbps and the download bandwidth is set to 20 Mbps. Both have a range of [0 - 1024].

In this example, the throughput rate for the Guest SSID has been limited to 10 Mbps upstream and 20 Mbps downstream.

Wi-Fi Multimedia and Quality of Service

Wireless networks are a shared medium, and you must make sure that critical latency-sensitive applications, such as voice traffic or video streaming, have priority over other applications.

Quality of service (QoS) prioritizes different classes of traffic throughout the wireless network. Wi-Fi Multimedia (WMM) admission control tags different types of traffic and maps them to different queues with custom WMM parameters. The WMM Access Categories, together with their corresponding identifying values, are described in this table.

WMM Access Categories			
Binary	802.1p Priority	WMM Access Category	Traffic Type
001	1	AC_BK	Background
010	2	AC_BK	Background
000	0	AC_BE	Best Effort
011	3	AC_BE	Best Effort
100	4	AC_VI	Video
101	5	AC_VI	Video
110	6	AC_VO	Voice
111	7	AC_VO	Voice

While some applications and devices can correctly tag packets for prioritization as they travel through the network, most traffic is transmitted as best effort (AC_BE). With a large amount of available capacity, this does not create an issue. But in enterprise wireless networks there are many use cases where channels operate at high levels of utilization, and you must correctly prioritize traffic for latency-sensitive applications such as voice and real-time video for solid application performance and a high quality user experience.

Inbound traffic from the Internet is transmitted as best effort, even if it originally was tagged as voice (AC_VO) before traversing the Internet, and network components, such as switches, routers and APs, must be able to identify, tag, and prioritize traffic.

End-to-End QoS

For optimal QoS, you must implement it end-to-end throughout the entire network. All components along the path must apply packet tagging.

WatchGuard APs use WMM on the wireless side, and DSCP (DiffServ Code Point) and 802.1p tagging for traffic destined for upstream networks on the wired side. DSCP/802.1p tagging guarantees appropriate delivery on the wired side of the network. We recommend that you enable QoS if you support voice or real-time video applications on your network.

To configure QoS settings:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Traffic Shaping & QoS** tab.
5. Select the **QoS** check box.
6. Configure your QoS settings as required. For more information on QoS configuration, see the *WatchGuard Wi-Fi Cloud Help*.
7. Save the SSID settings.

The screenshot shows the 'My SSID' configuration page with tabs for Basic, Security, Network, RF Optimization, and Traffic Shaping & QoS. The 'Traffic Shaping & QoS' tab is selected and highlighted with a red box. Within this tab, the 'QoS' checkbox is checked and highlighted with a red box. Below this, there are several settings: 'Enforce WMM Admission Control' is unchecked; 'SSID Priority' is set to 'Voice'; 'Priority Type' has 'Ceiling' selected; 'Downstream Mapping' is set to 'DSCP'; and 'Upstream Marking' has '802.1p Marking' checked, with 'DSCP/TOS Marking' unchecked and 'DSCP' and 'TOS' radio buttons below it.

Application Visibility and Control

Application Visibility provides real-time, Layer 7 application classification and meta data extraction for network traffic. Application Visibility uses a combination of application classification and inspection techniques to deliver industry leading scope and accuracy. Application Visibility automatically classifies thousands of popular applications.

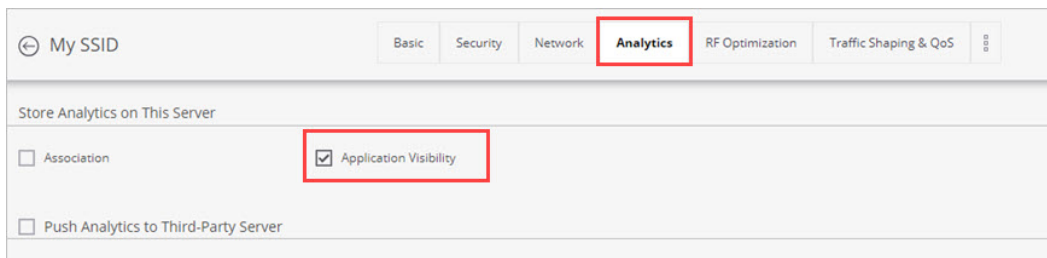
Application Visibility enables you to see the applications used by each client and provides a global view of what applications are used on the network. You can block, rate limit, or prioritize (tag) individual applications.

You can enable Application Visibility in an SSID Profile (802.11ac Wave 2 APs only).

If you do not already have a firewall or network appliance that has application control features, we recommend you enable Application Visibility on all SSIDs that could be used for voice or video traffic. This can improve application performance and can enhance the quality of experience for end users.

To enable Application Visibility on an SSID:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID Profile.
4. Select the **Analytics** tab.
5. Select the **Application Visibility** check box.
6. Save the SSID settings.



The screenshot shows the 'My SSID' configuration page with the 'Analytics' tab selected. Under the 'Store Analytics on This Server' section, the 'Application Visibility' checkbox is checked and highlighted with a red box. Other options include 'Association' and 'Push Analytics to Third-Party Server', both of which are unchecked. The 'Analytics' tab is also highlighted with a red box in the top navigation bar.

Basic	Security	Network	Analytics	RF Optimization	Traffic Shaping & QoS	More
Store Analytics on This Server						
<input type="checkbox"/> Association	<input checked="" type="checkbox"/> Application Visibility					
<input type="checkbox"/> Push Analytics to Third-Party Server						

Application Firewall

When Application Visibility is enabled, you can use the Application Firewall to create rules and control application use on an SSID.



The default application firewall rule is to block all applications.

To enable the Application Firewall:

1. Open Discover.
2. Select **Configure > WiFi**.
3. Select an SSID profile.
Make sure that Application Visibility is enabled on the SSID Profile.
4. Select the **Access Control** tab.
5. Select the **Application Firewall Rules** check box.
6. Configure your rules.
7. Save the SSID settings.

My SSID

Basic Security Network **Access Control** Analytics RF Optimization Traffic Shaping & QoS

▼ Show Less

☐ Layer 3-4 Firewall Rules

☒ Application Firewall Rules

Rule Name * Category *
Select Category

Action
Allow

+

-

Default Rule

Action
Block

WIPS (Wireless Intrusion Prevention System)

WatchGuard APs can run in these modes:

- Wi-Fi Access point only
- Wi-Fi Access point with background scanning and wireless security features enabled
- Dedicated WIPS sensor

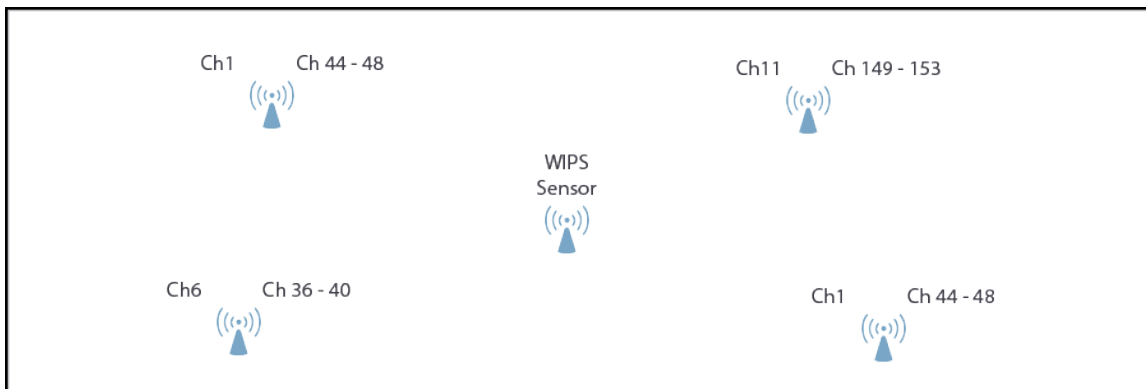
You can deploy APs in Wi-Fi access point mode with background scanning. This option provides robust protection for many Wi-Fi threats.

Video streaming and voice application performance are another important consideration. APs that have background scanning enabled must periodically scan all channels. This means that the AP must temporarily leave the channel where the AP is servicing clients. For typical data traffic, such as web browsing or email, the latency that results from channel scanning does not create issues. However, for real-time applications, this latency is not acceptable.

On 802.11ac Wave 2 APs you can enable VoIP-aware scanning to perform the functions of background scanning but optimize the scanning for high-priority real-time traffic. If you enable VoIP-aware scanning, make sure that SSIDs added to this radio have the Application Visibility option enabled for traffic detection.

For comprehensive protection against Wi-Fi threats, we recommend you use dedicated WIPS sensors. For example, if you need to prevent your wireless clients from connecting to an unauthorized personal hotspot, your deployment must include a WIPS sensor.

You can configure dual-radio APs as dedicated WIPS sensors that dedicate both radios to WIPS scanning and do not broadcast Wi-Fi. Tri-radio devices such as the AP225W, AP325, and AP420 have a dedicated WIPS sensor on the third radio.



We recommend you deploy a dedicated WIPS sensor for every three to five Wi-Fi access points.

- Place your WIPS sensors to provide full coverage over your Wi-Fi airspace, but do not install them too close to your existing APs to avoid interference.
- Make sure there is some overlap in the coverage area so that at least two sensors are active in the same area in the event of multiple threats.

Some AP models must use full PoE+ power or be connected to a power adapter for the third WIPS scanning radio to be fully effective. Lower PoE power results in reduced performance and effectiveness of WIPS scanning and intrusion prevention functions. For more information, see the "AP Power Requirements" section in [Wired Network Best Practices](#).

For detailed information on how to configure Wi-Fi Cloud WIPS to meet the requirements of a Trusted Wireless Environment, see [Create a Trusted Wireless Environment with WIPS](#).

You can test your own wireless network security measures to see if they are able to detect and prevent the six known threats identified by the Trusted Wireless Environment. For more information, see the [Trusted Wireless Environment Test Guide](#).

Summary of Wireless Network Recommendations

This table provides a summary of the recommendations for a wireless network deployment.

Feature	Default	Recommended	Notes
SSID Profile Options			
SSIDs	0	Limit number of SSIDs to 6 per AP	WatchGuard APs support up to 8 SSIDs per radio, or 16 SSIDs per AP.
SSID Network Mode	Bridge	Bridge	Consider NAT only for small remote site deployments.
Application Visibility	Disabled	Enabled	You must also enable QoS in your end-to-end switching infrastructure.
Bonjour Gateway	Disabled	Enabled	
Min Unicast Data Rate	2.4 GHz - 1 Mbps 5 GHz - 6 Mbps	24 Mbps	Removing supported data rates can cause client interoperability issues.
Min Multicast, Broadcast, and Management Rate	2.4 GHz - 1 Mbps 5 GHz - 6 Mbps	24 Mbps	This rate should be equal to or greater than Min Unicast (Association) Data Rate.
Traffic Shaping	Disabled	Enable for Guest wireless network	
Smart Client Load Balancing	Disabled	Enabled	
Smart Steering	Disabled	Enabled with default settings	Consider leaving Smart Steering disabled in environments that support voice traffic.
Minimum Association RSSI	-65 dBm	-65 dBm	Wireless network should be designed for -62 dBm or greater throughout the entire deployment.
802.11k and 802.11v	Disabled	Enabled	

Feature	Default	Recommended	Notes
Proxy ARP	Disabled	Enabled	
Broadcast and Multicast Suppression	Disabled	Enabled	A function of the WatchGuard AP layer 2 Firewall.
Reliable Multicast Delivery	Disabled	Enabled	AP converts multicast to unicast and uses IGMP Snooping to build multicast group forwarding tables at the AP.
Device and Radio Settings			
Channel Width	20/40/80 MHz	20/40/80 MHz for 802.11ac	Use 20/40 MHz if DFS channels are not available.
AP Mode	Wi-Fi only	Wi-Fi only or WIPS Sensor	Deploy one full-time WIPS sensor for every 3 to 5 Wi-Fi only APs for maximum AP performance and WIPS effectiveness.
Auto Channel Selection / Dynamic Channel Selection	Enabled	Enabled or Disabled with a Static Channel Plan	Depends on the environment and preference of your network deployment engineers.
AP Power	Auto Power	Auto Power or Static Power Plan Classroom: 5 GHz: 8 - 16 dBm 2.4 GHz: 4 - 10 dBm Auditorium/Lecture Hall: 5 GHz: 5 - 12 dBm 2.4 GHz: 3 - 10 dBm	Depends on the environment and preference of network deployment engineers.

Wired Network Best Practices

This section provides suggestions on how to deploy a wired network infrastructure to support a high performance 802.11ac wireless deployment for enterprise environments.

AP Power Requirements

Not all WatchGuard APs have the same power requirements. Some models, such as the AP125 or AP225W, are fully functional with standard Power over Ethernet (PoE, 802.3af). For most deployments, we recommend you install switches that support PoE+ (802.3at), even if you currently do not have plans to deploy an AP that requires PoE+. The use of PoE+ switches enables you to support Wave 2 APs.

Model	Description	Recommended Use	Power	Notes
AP120 (Legacy model)	Dual radio, 802.11ac Wave 1, 2x2, Indoor	Low density / throughput areas	PoE	Fully functional with PoE
AP320 (Legacy model)	Dual radio, 802.11ac Wave 1, 3x3, Indoor	Medium to high density / throughput areas	PoE	Fully functional with PoE
AP322 (Legacy model)	Dual radio, 802.11ac Wave 1, 3x3, Outdoor	Outdoors	PoE+	Requires PoE+
AP125	Dual radio, 802.11ac Wave 2, 2x2, Indoor	Low density / throughput areas	PoE	Fully functional with PoE
AP225W	Tri-radio, 802.11ac Wave 2, 2x2, Indoor, Wall plate	Low / medium density / throughput areas	PoE	Fully functional with PoE
AP325	Tri-radio, 802.11ac Wave 2, 2x2, Indoor	Low / medium density / throughput areas	PoE+	Requires PoE+
AP327X	Dual radio, 802.11ac Wave 2 2x2, Outdoor	Outdoors	PoE+	Requires PoE+
AP420	Tri-radio, 802.11ac Wave 2, 4x4, Indoor	High density / throughput areas	PoE+	Requires PoE+

AP325 and AP420 models must use full PoE+ power or be connected to a power adapter for the third WIPS scanning radio to be fully effective. Lower PoE power results in reduced performance and effectiveness of WIPS scanning and intrusion prevention functions.

In addition, make sure that LLDP-capable switches provide appropriate PoE+ power for APs:

- You must enable LLDP on the switch
- Disable static allocation of maximum power of 30W (if previously configured)

For more information, see [WatchGuard APs and PoE+ power with switches and LLDP](#).

AP Uplink Capacity

In lab tests, the dual band throughput of 802.11ac Wave 1 APs has exceeded 1 Gbps. The maximum theoretical data rate in the 5 GHz band is 1.3 Gbps (802.11ac 3x3). In the 2.4 GHz band (802.11n 3x3) it is 450 Mbps.

In production, throughput rarely exceeds the 1 Gbps barrier. With Wave 2 APs, such as the AP420 that supports 4 spatial streams with a combined maximum data rate of 2.3 Gbps (1.7 Mbps for 5 GHz and 600 Mbps for 2.4 GHz), it is likely that throughput in a production environment can exceed the 1 Gbps throughput barrier in some use cases.

Link Aggregation

WatchGuard recommends that you enable this feature in a device template so that you can connect two Ethernet cables to each supported AP and a compatible switch with link aggregation enabled. The AP can then load balance upstream traffic across an aggregated 2 Gbps connection. Both links should use CAT6 Ethernet cabling.

AP Cabling

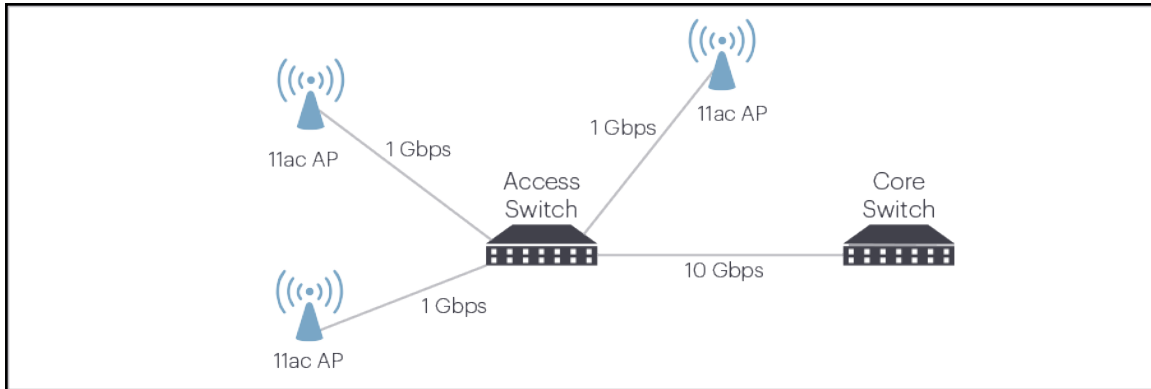
At a minimum, 802.11ac APs require Cat5e cables.

For fully 802.11ac Wave 2 deployments, we recommend that you deploy Cat6a cables because Wave 2 APs have Ethernet ports that support rates greater than 1 Gbps.

Cable Category Reference				
Cable Category	Max Data Rate	Bandwidth	Max Distance (Meters)	Max Distance (Feet)
Cat 5	100 Mbps	100 MHz	100 Meters	328 Feet
Cat 5e	1 Gbps	100 MHz	50 Meters	164 Feet
Cat 6	10 Gbps	250 MHz	50 Meters	164 Feet
Cat 6a	10 Gbps	500 MHz	100 Meters	328 Feet
Cat 7	10 Gbps	600 MHz	100 Meters	328 Feet

Access Network Uplink

You must correctly design the switching infrastructure to take full advantage of the increased throughput capacity of 802.11ac APs. To make sure that there are no network bottlenecks, you must correctly size the network from the access and distribution switches to the core switch.



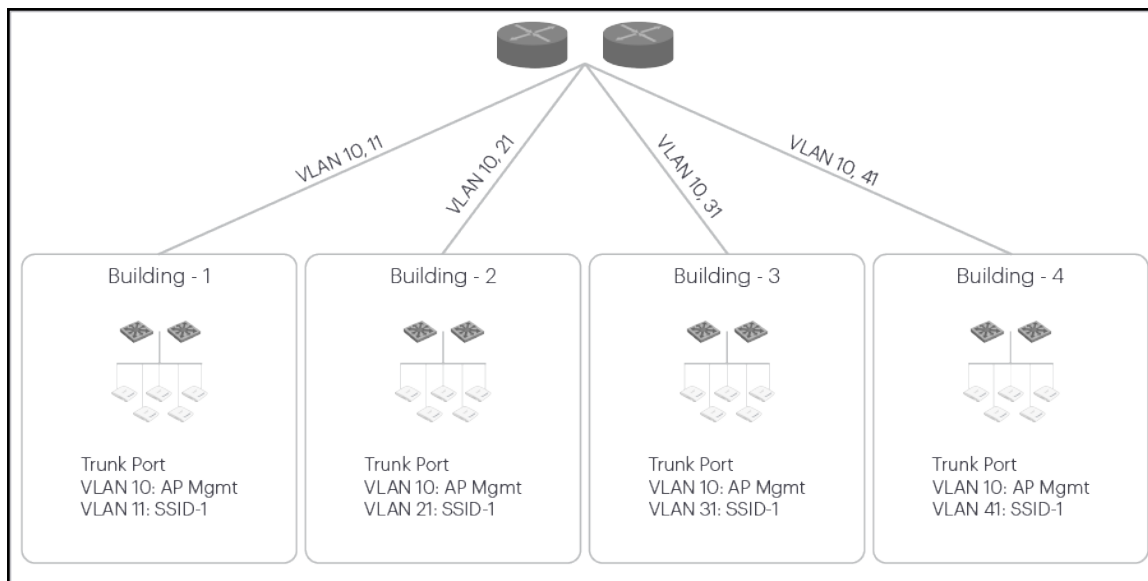
Here is a summary of the recommended uplink capacities for 802.11ac wireless networks:

- 1 Gbps for Wave 1 APs to the access/edge switch
- Consider 2 x 1 Gbps for Wave 2 APs to the access/edge switch
- 10 Gbps from the access switch to the distribution switch
- Consider dual-homed/redundant 10 Gbps uplink between the access and distribution switches
- Multi-homed/redundant 10 Gbps between core switches

VLAN Design

With WatchGuard Wi-Fi Cloud, it is not necessary to tunnel traffic through VLANs to a wireless controller located in the core of the network. This enables you to configure VLANs at the access switch layer of the network.

In this example, each building has a unique VLAN configured for SSID-1. You can restrict a VLAN to a single building to reduce the amount of broadcast and multicast traffic in the VLAN, and enable seamless roaming in the building.



Jumbo Frames

With the enhanced frame aggregation capabilities in the 802.11ac standard, the switching network must support jumbo frames to benefit from frame aggregation. If Jumbo Frame support is not enabled end-to-end in your network, fragmentation can occur in the network path, which can adversely affect performance.

Summary of Wired Network Recommendations

This table provides a summary of the recommendations for your wired network.

Feature	Minimum	Recommended	Notes
AP Power	PoE	PoE+	AP322, AP325, AP327X, and AP420 devices require PoE+ LLDP enabled on switches to ensure PoE+ connectivity
AP Uplink Capacity	1 Gbps	Consider 2 x 1 Gbps for link aggregation	
Ethernet Cabling	Cat5e	Cat6a	
Access Network Uplink Capacity	10 Gbps	2 x 10 Gbps	Multi-homed / Fault Tolerant
VLAN Design	Wireless network VLANs on access switches	Route at the distribution layer	
Jumbo Frames	A-MPDU and A-MSDU frame aggregation enabled on APs	Enable support for Jumbo Frames throughout the entire switching infrastructure	
QoS	Make sure all switches, from access switches to core switches, honor QoS tags	Deploy switches and routers that support Application Visibility and Control (AVC)	

Network Services Best Practices

This table provides recommendations for network service configuration to support a WatchGuard Wi-Fi Cloud deployment in an enterprise environment.

Service	Recommended	Notes
DHCP	Use the current network DHCP servers.	
DNS	Use the current network DNS services.	
Proxy	Configure proxy bypass rules to allow AP to cloud management traffic.	<p>All management traffic from the access points to Wi-Fi Cloud must be configured to bypass proxies while preventing unfiltered user access to the Internet.</p> <p>You can use a WatchGuard Firebox to configure policies for Wi-Fi Cloud traffic and bypass proxies. Predefined policies are available for this purpose. If your Firebox runs Fireware v11.11.4 or higher, the Firebox configuration file includes the predefined <i>WG-Cloud-Managed-WiFi</i> packet filter policy that you can add to the configuration to enable traffic over the ports required for WatchGuard Wi-Fi Cloud domains.</p>
Firewall	<p>You must allow this traffic on your firewall:</p> <ul style="list-style-type: none">■ Port 3851 (UDP) outbound■ Port 3852 (UDP) outbound for APs configured in CIP mode■ Port 80 (TCP) outbound / stateful inbound■ Port 443 (TCP) outbound / stateful inbound	<p>These are the required ports for WatchGuard APs to communicate with WatchGuard Wi-Fi Cloud at these domains:</p> <p>*.cloudwifi.com</p> <p>redirector.online.spectraguard.net</p>
NAT	Use the current network NAT solution.	Consider enabling NAT on the AP for small remote sites.

Service	Recommended	Notes
Traffic Shaping and QoS	Apply traffic shaping and QoS to traffic inbound from Internet.	
Content Filtering	Use the current network content filter solution.	Consider content filtering on the AP for small remote sites.
RADIUS	Use the current network RADIUS solution.	

AP Placement and Channel Plan Best Practices

With the information in the capacity planning section of this guide, you can determine how many APs are required for specific deployment use cases. In this section, you determine where to put the APs and the wireless channels to use.

Wireless Signal Strength and Noise Levels

To make sure that all users in your environment receive a strong wireless signal, consider these guidelines when you install your WatchGuard APs.

Signal Strength

The signal strength is the wireless signal power level received by the wireless client.

- Strong signal strength results in more reliable connections and higher speeds.
- Signal strength is represented in dBm format (0 to -100). This is the power ratio in decibels (dB) of the measured power referenced to one milliwatt.
- The closer the value is to 0, the stronger the signal. For example, -41 dBm is a stronger signal than -61 dBm.

Noise Level

The noise level indicates the amount of background noise in your environment.

- If the noise level is too high, it can degrade the strength and performance of your wireless signal.
- Noise level is measured in dBm format (0 to -100). This is the power ratio in decibels (dB) of the measured power referenced to one milliwatt.
- The closer the value to 0, the greater the noise level.
- Negative values indicate less background noise. For example, -96 dBm is a lower noise level than -20 dBm.

Signal to Noise Ratio

The signal-to-noise ratio (SNR) is the ratio between the signal strength and the noise level.

- This value is represented as a dB value.
- In general, your signal-to-noise ratio should be +25 dB or higher. Values lower than +25 dB result in poor performance and speeds.

For example:

- If you have a -41 dBm signal strength, and a -50 dBm noise level, this results in a poor signal-to-noise ratio of +9 dB.
- If you have a -41 dBm signal strength, and a -96 dBm noise level, this results in an excellent signal-to-noise ratio of +55 dB.

RF Interference

Interference caused by Wi-Fi or non-Wi-Fi devices can greatly reduce performance of wireless networks. To optimize the performance of your wireless network you must be able to identify, locate and avoid sources of interference. To help you to identify sources of interference, you can perform a spectrum analysis during the pre-installation and post-deployment phases .

Wi-Fi Interference Sources

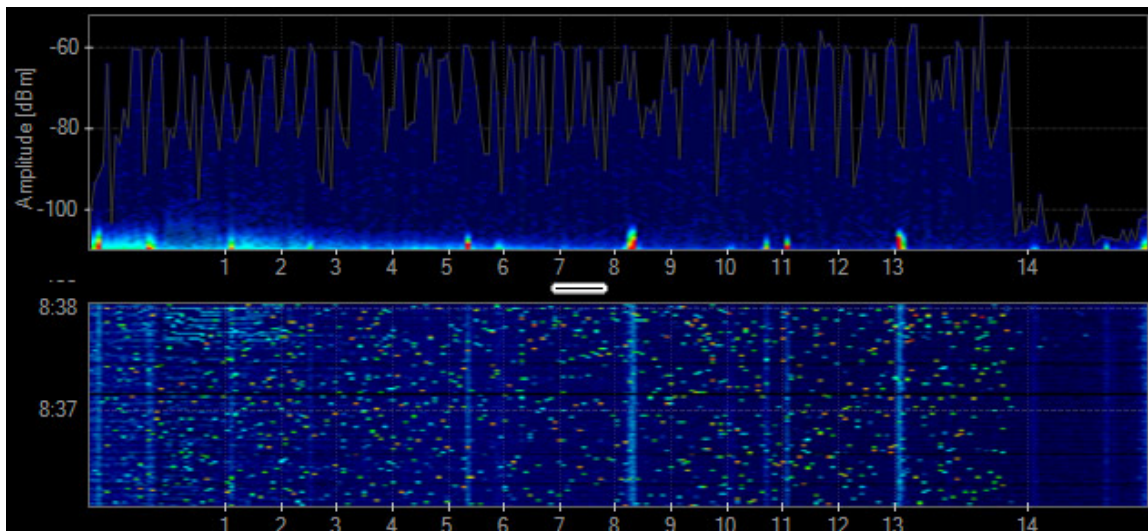
- Personal hotspots
- Malfunctioning clients
- Poorly designed wireless network or misconfiguration
- Neighborhood APs and clients external to your network

Non-Wi-Fi Interference Sources

- Video game controllers
- Microwave ovens
- Security cameras
- ZigBee devices
- Cordless phones
- Bluetooth devices

Microsoft Xbox Game Controller

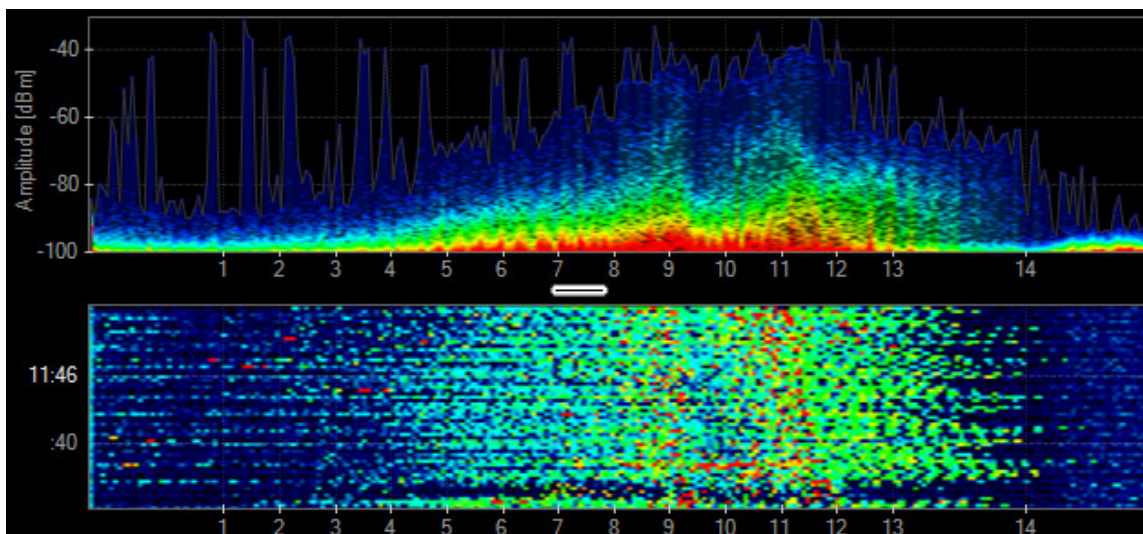
Game controllers for the Microsoft Xbox use non-Wi-Fi 2.4 GHz wireless technology. Game controllers use their own frequencies and use frequency-hopping. Though the channel utilization of these devices is quite low, these controllers can adversely affect Wi-Fi performance in the 2.4 GHz band.



Xbox game controller frequency spectrum chart. Source: Metageek

Microwave Oven

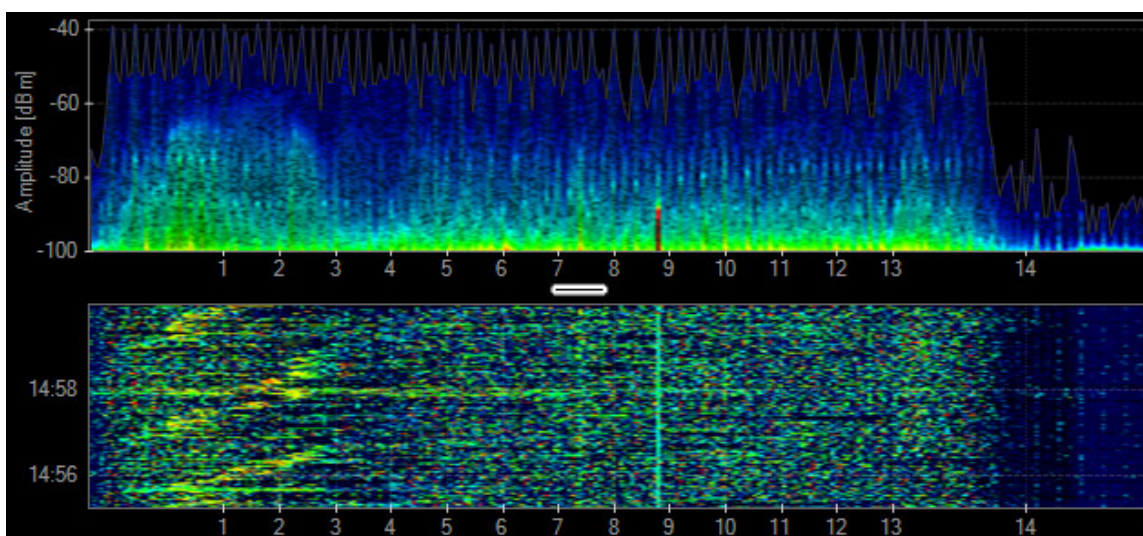
Microwave ovens operate in the upper channels of the 2.4 GHz band. Microwave ovens have been known to have severe impacts on performance for nearby APs and clients operating on channels 6 to 13. Do not put APs near microwave ovens, but when it is unavoidable, we recommend you use channel 1 for the 2.4 GHz radio.



Microwave oven frequency spectrum chart. Source: Metageek

Bluetooth

Bluetooth devices are frequency hoppers that can affect all channels in the 2.4 GHz band. Fortunately, Bluetooth devices do not stay on a single frequency for very long and they operate with relatively low power, so their impact is limited.



Bluetooth frequency spectrum chart. Source: Metageek

Wi-Fi Cloud Smart Spectrum

The Smart Spectrum feature in WatchGuard Wi-Fi Cloud detects and identifies interference sources, both Wi-Fi and non-Wi-Fi. The interference data is collected by the DCS (Dynamic Channel Selection) algorithm for more informed AP channel changes that result in improved overall network performance and user experience.

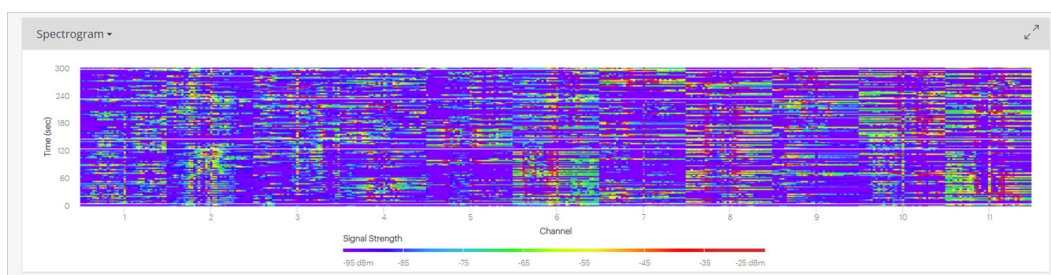
When you enable ACD/DCS (auto channel) selection, APs select channels to avoid both Wi-Fi and non-Wi-Fi interference. It is preferable that wireless networks not routinely change their channel plan because channel plan changes can be disruptive to the wireless network.

Unwanted sources of interference from devices such as rogue APs, cordless phones, and non-Wi-Fi cameras can reduce wireless network performance. To mitigate this issue, provide a spectrum policy that informs all users about the types of devices that are not permitted at your deployment site.

Additional sources of interference are even more of a problem for static channel plans, (where auto channel selection is disabled), because manual intervention is required to locate and remove the source of the interference or to change the channel plan to avoid the interference. We recommend you have a spectrum policy to help minimize wireless network disruptions caused by sources of interference introduced into your network.

Spectrum Analysis with Discover

In WatchGuard Discover, you can perform Spectrum Analysis that helps you detect various types of interference, non Wi-Fi interference, or interference that can also be transient in nature that decreases the performance of your wireless network. Spectrum analysis enables you to visualize the radio frequencies operating in your area and determine the strength of the detected signals.



Signal Strength, Channel Width, and QAM

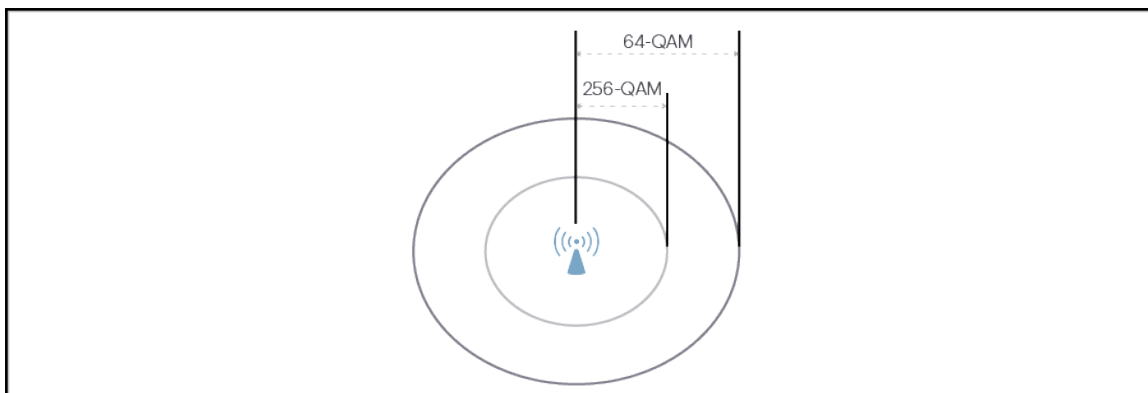
This table shows the approximate signal strengths required to support MCS rates for various channel widths. 256-QAM requires higher signal strengths than 64-QAM because of the greater constellation density required to support 256-QAM. However, wider channels also require higher levels of signal strength compared to narrow channels to support a given modulation scheme.

For example, 64-QAM/MCS-7 requires -62 dBm for 40 MHz channels, but the requirement jumps to -58 dBm for 80 MHz channels. To design a network to support 256-QAM/MCS-9 with 80 MHz channels pervasively, requires a signal strength of -52 dBm or higher throughout the deployment. This means that

APs should be located every 30 to 50 feet, depending on the environment, clients, and AP capabilities. While there may be high density and high /throughput use cases (such as an auditorium) where designing for 256-QAM is recommended, most high density deployments are designed to support 64-QAM pervasively.

Signal Strengths Required to Support MCS Rates for Various Channel Widths					
Modulation Scheme	20 MHz	40 MHz	80 MHz	80+80 MHz	160 MHz
11ac 64-QAM/MCS-7	-64 dBm	-62 dBm	-58 dBm	-55 dBm	-55 dBm
11ac 256-QAM/MCS-8	-59 dBm	-56 dBm	-53 dBm	-50 dBm	-50 dBm
11ac 256-QAM/MCS-9	-58 dBm	-54 dBm	-52 dBm	-49 dBm	-49 dBm

Higher density modulation requires higher levels of signal strength, and wider channels require higher signal strength compared to narrower channels. As a result, the cell size for an AP that supports 256-QAM is much smaller than that of an AP that supports 64-QAM, as shown in this diagram.



Predictive Site Survey

Use a predictive site survey software application to develop an AP placement plan estimate coverage and capacity. You can use a predictive site survey planning application to generate a recommended AP placement and channel plan, including coverage, SNR, and interference information to help with your deployment.

You must provide input on these factors for correct capacity planning:

- Client types and quantity (currently in use and anticipated growth)
- Applications (currently in use and anticipated growth) and streaming media requirements
- Design for capacity
- High-quality floor maps
- Precise scale for the floor plan
- Consideration of possible RF leaks between floors

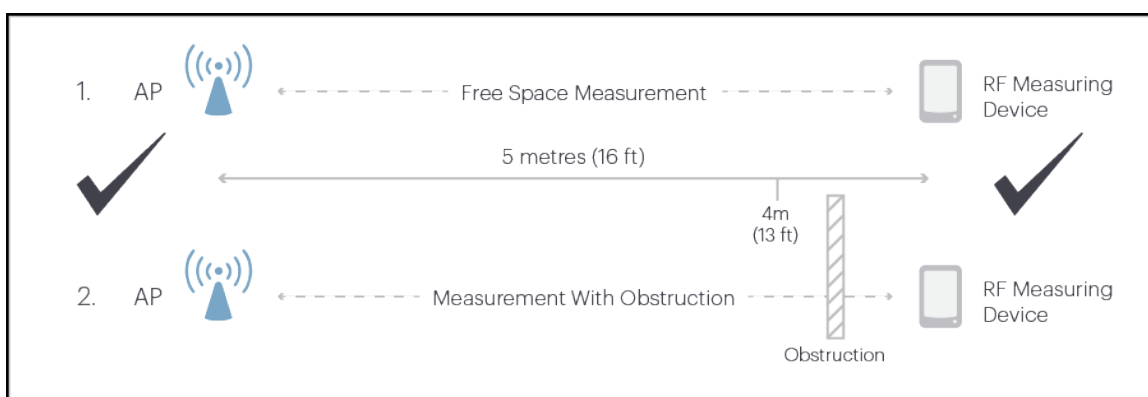
WatchGuard provides to partners a *Wi-Fi Customer Requirements Questionnaire* to assist in creating predictive site surveys. For more information, log in to your partner account on the WatchGuard web site and go to **Product > Selling Secure Wi-Fi**.

Indoor Attenuation Reference

To make sure you have an accurate predictive site survey, measure the actual attenuation values for obstructions within the deployment site. You can use these attenuation values in your site survey. To measure attenuation values, you must use an AP and a smart phone with an application such as *WiFi Analyzer*.

To perform the measurement, check the signal level detected by the client when the client and AP are 5 meters apart with a clear line of sight (LoS). Then, check the signal level again at the same distance with the obstruction between the AP and the smart phone.

The difference between the LoS (line of sight) reading and the second reading is the measure of attenuation level for the obstruction. The attenuation values you obtain can improve the accuracy of your predictive site survey.



Example:

- Measurement 1: 5 Meters LoS = -54 dBm
- Measurement 2: 5 Meters behind obstruction = -57 dBm
- Obstruction Attenuation = 3 dB

This table shows the estimated values of attenuation for common materials found in typical deployments. Note the variability in attenuation for a specific type of material (for example, concrete and brick wall +/- 10 dB). Precise attenuation values produce a more accurate predictive site survey.

Attenuation Estimations		
RF Attenuators	Estimated Attenuation in 2.4 GHz	Estimated Attenuation in 5 GHz
Steel door	16 dB (+/- 3 dB)	28 dB (+/- 3 dB)
Concrete or brick wall	12 dB (+/- 6 dB)	20 dB (+/- 10 dB)
Coated or double-pane	12 dB (+/- 1 dB)	20 dB (+/- 1 dB)
Cubicle wall	4 dB (+/- 1 dB)	6 dB (+/- 2 dB)

Attenuation Estimations		
Wood door	4 dB (+/- 1 dB)	6 dB (+/- 1 dB)
Glass or window (not tinted)	3 dB (+/- 1 dB)	7 dB (+/- 1 dB)
Drywall (interior)	3 dB (+/- 1 dB)	4 dB (+/- 1 dB)
Ceiling tiles, curtains, blinds	1 dB (+/- .5 dB)	2 dB (+/- 1 dB)

Rule of 10s and 3s

You can increase or decrease power due to several factors such as antenna gain and attenuation loss due to distance between APs and clients

- If you lose -3 dB, you lose 1/2 your original power
- If you gain +3 dB, you gain 2x your original power
- If you lose -10 dB, this is 1/10 your original power
- If you gain +10dB, you have 10x your original power

One-for-One AP Replacement

Before you choose a one-for-one AP replacement approach, make sure these conditions are true:

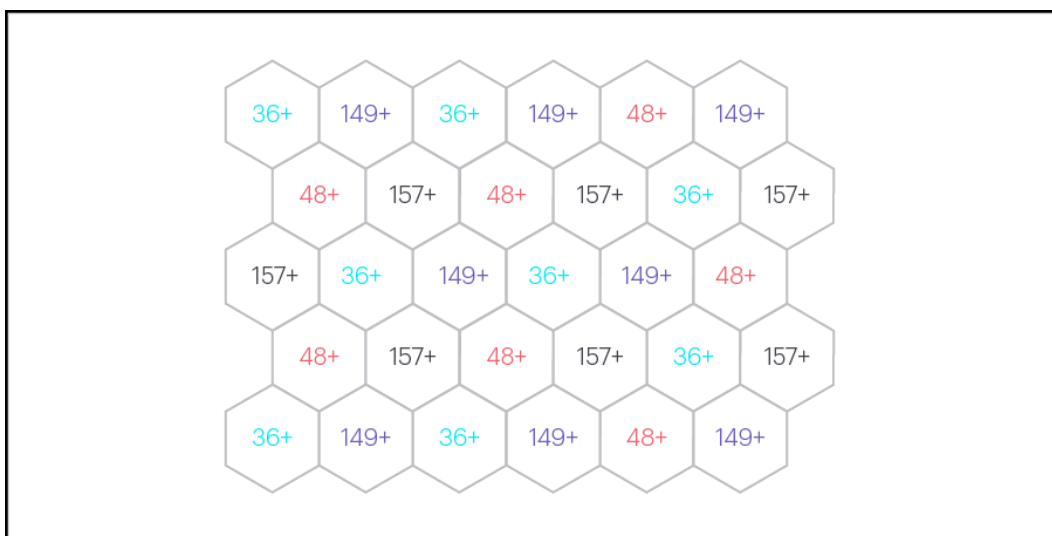
- The current wireless network provides correct coverage everywhere (for example, -62 dBm).
- All clients can detect two to three APs in all locations.
- The current network is designed for capacity.
- All applications perform correctly.
- The environment has remained the same (for example, no building renovations) since the existing AP placement plan was created.
- The current network is designed for 5 GHz.
- All clients can roam successfully.

Avoid Self Induced CCI in 2.4 GHz

Even if DFS channels are not used, 5 GHz channels outnumber 2.4 GHz channels by a wide margin. This means that if both 5 GHz and 2.4 GHz radios are active on all APs in a network designed for capacity, there is a high probability that the APs could create harmful co-channel interference (CCI) in the 2.4 GHz band. Another factor is that 2.4 GHz frequencies provide greater coverage range than 5 GHz frequencies. To minimize the amount of self-induced CCI in the 2.4 GHz band, we recommend you disable 2.4 GHz radios on some of the deployed APs .

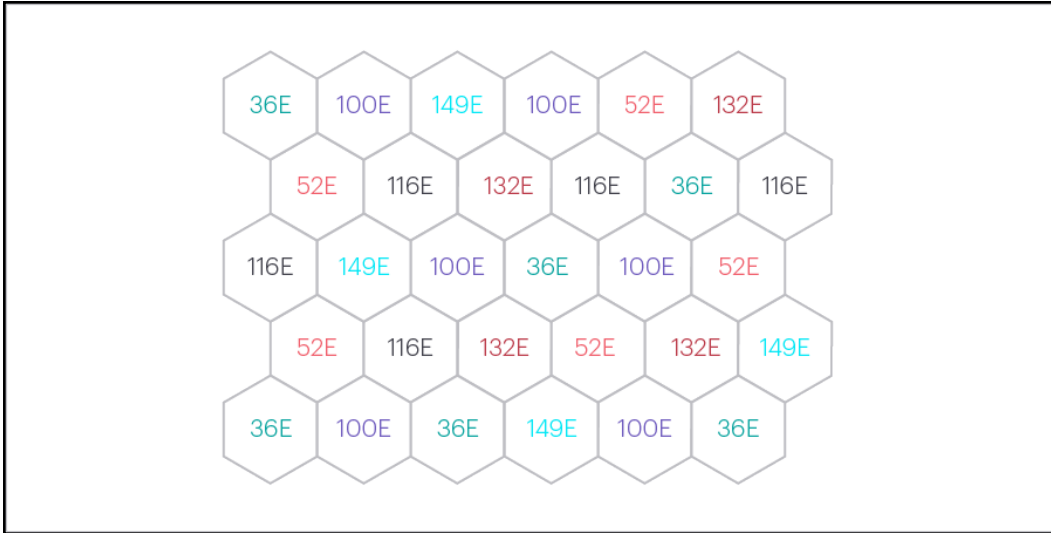
40 MHz Channel Plan

The diagram below is an example of a 40 MHz channel plan that does not use DFS channels. In the US, as well as in several other regions, there are only four non-overlapping 40 MHz channels available if DFS channels are not used. The example plan minimizes CCI because adjacent APs do not use the same frequencies.



80 MHz Channel Plan

This is an example of an 80 MHz channel plan that uses DFS channels. In the US, as well as in several other regions, there are six non-overlapping 80 MHz channels available if DFS channels are used. As with the 40 MHz plan, the example plan minimizes CCI because adjacent APs do not use the same frequencies.



AP Mounting Recommendations

WatchGuard APs for indoor use are usually mounted on walls or ceilings. Outdoor APs are usually mounted on walls and poles.

More information about mounting options are provided in the [WatchGuard AP Hardware Guides](#).

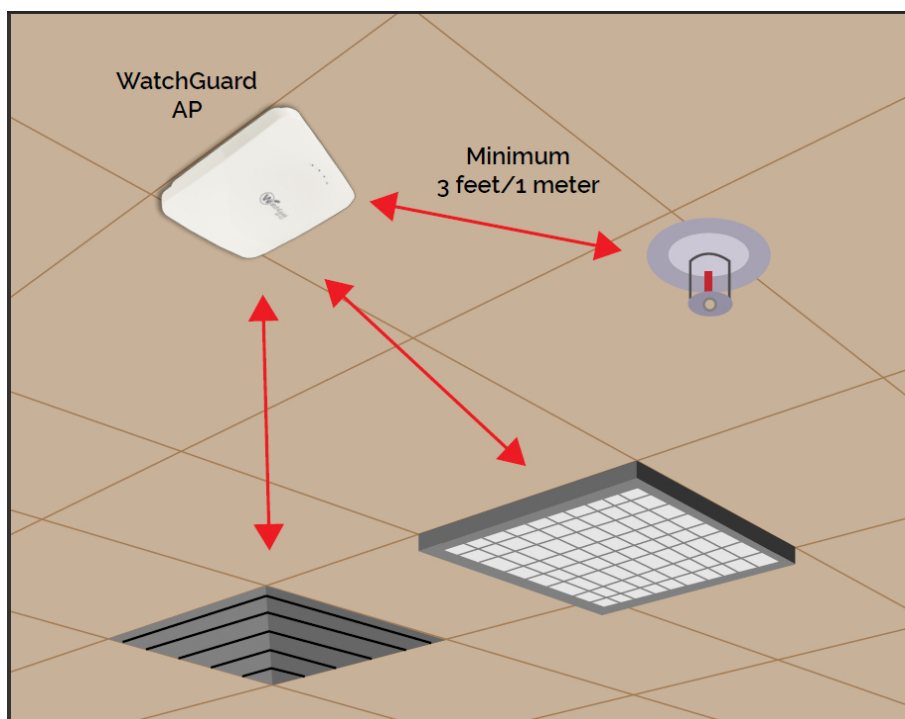
Information about WatchGuard AP antenna radiation patterns (internal and external) can be found in corresponding device data sheets located on the [WatchGuard website](#).

Wall Mount

While not as common as ceiling mounts, wall-mounted APs are also appropriate for most rooms. Wall-mounted APs can also be found in large rooms, such as auditoriums, where ceiling mounts are not practical because of ceiling height or accessibility. If you mount APs with a wall mount, consider the antenna radiation patterns, including back lobe patterns, of the AP model you deploy.

Ceiling Mount

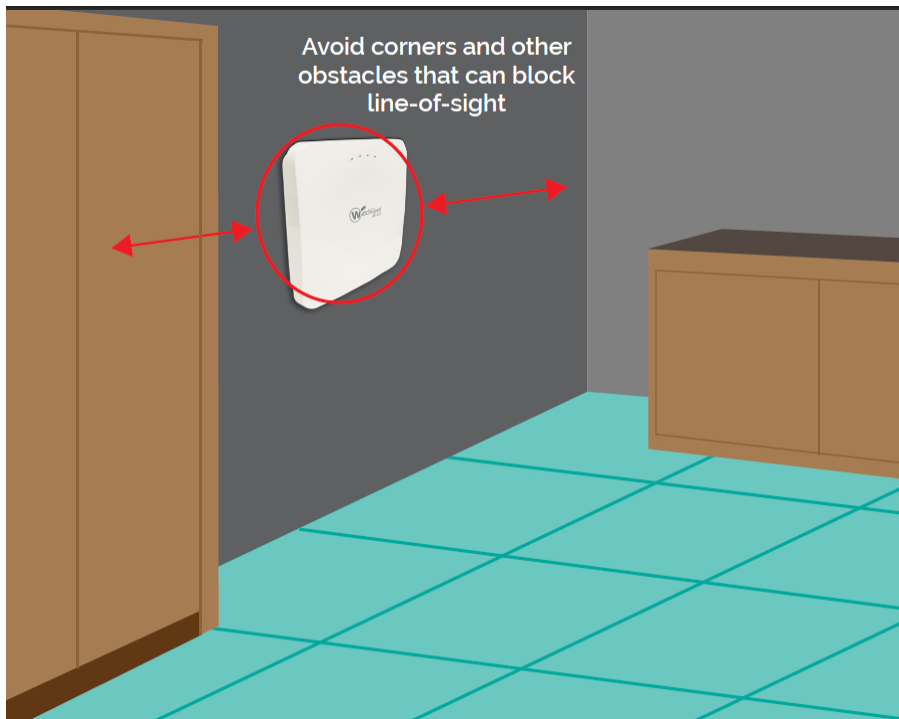
Most wireless network deployments use ceiling mounts. When you mount APs to a ceiling, it is preferable to mount APs below the ceiling. Do not hide APs above a dropped ceiling for aesthetic or physical security purposes. The ceiling space can include metallic structures such as pipes or AC ducts that can attenuate RF transmissions.



Structural Proximity and Electrical Interference

These factors can affect the reliability and performance of the wireless network:

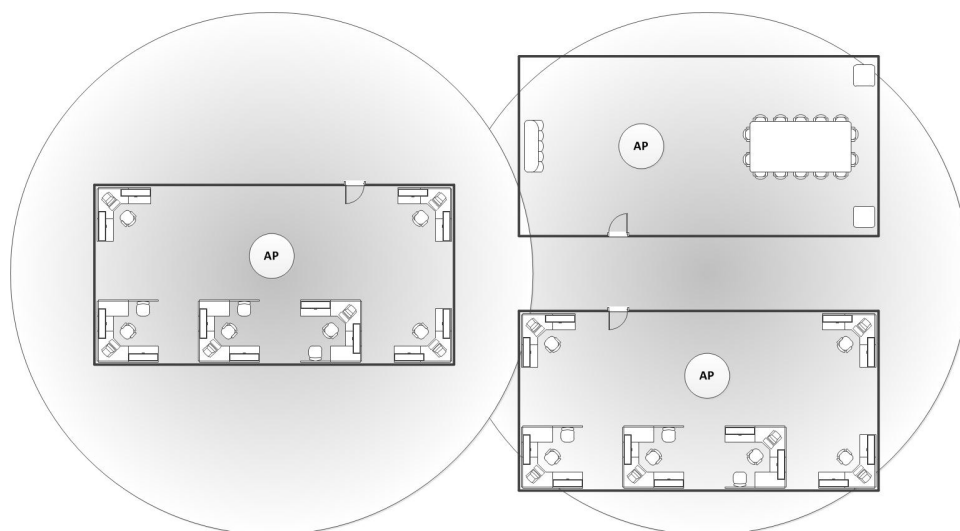
- Physical obstacles that can impede radio transmissions
- Radio frequency interference (RFI) from electronic devices and other radio sources
- Electromagnetic interference (EMI) from fluorescent bulbs, motors, and appliances
- Incorrect AP antenna placement
- Improper antenna selection
- Distances between access points and clients



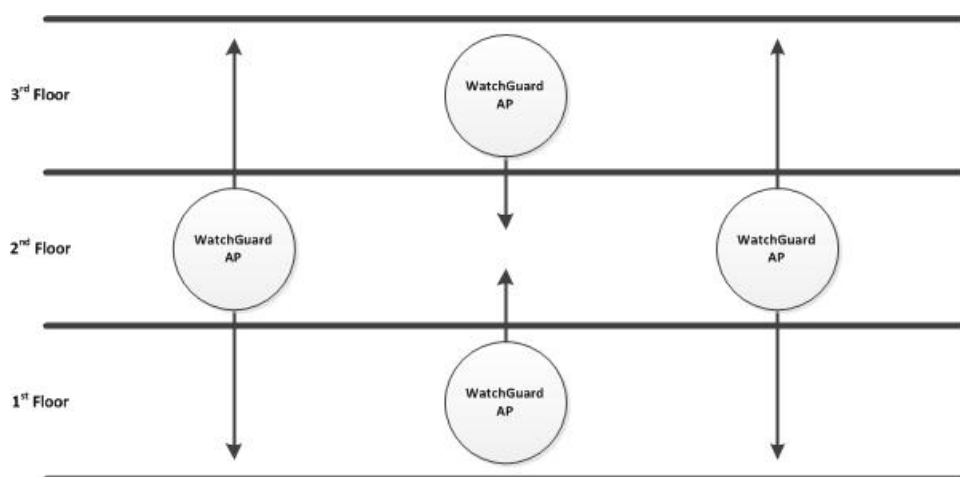
AP Placement

For full wireless coverage and to make sure that all clients on your environment receive a strong wireless signal, consider these guidelines for the location and placement of your WatchGuard APs:

- Install your APs in a central location away from any corners, walls, or other physical obstructions to provide maximum signal coverage.
- Install your APs in a high location to provide the overall best signal strength reception and performance for your wireless network. In general, one AP can cover up to approximately 2000 square feet, with variation based on the physical environment and wireless interference.
- Make sure you do not install an AP near any electronic devices that can interfere with the signal, such as televisions, microwave ovens, cordless phones, air conditioners, fans, or any other type of equipment that can cause signal interference.

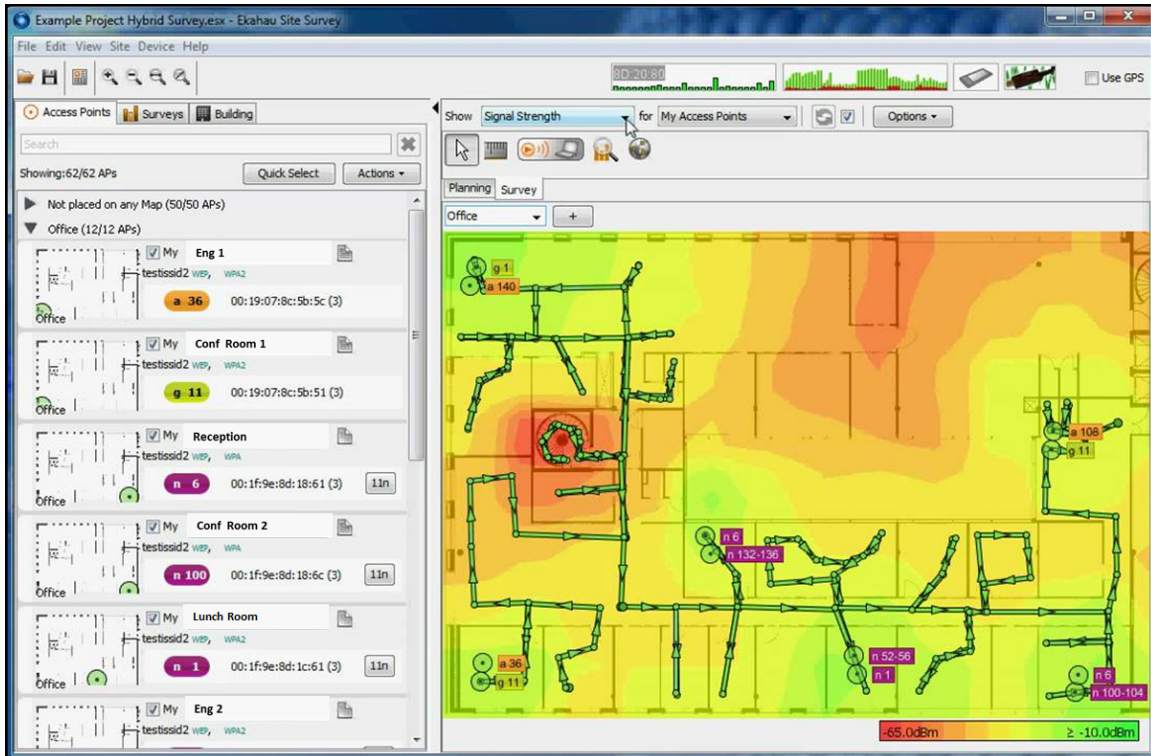


- When you install more than one AP, make sure to leave enough space between them to provide maximum coverage for your wireless network area of availability.
- For wireless coverage over many floors, you can stagger the placement of APs to cover both vertical and horizontal space.



Post-Deployment Validation Survey

There are many post-deployment site survey tools available. The Ekahau Site Survey (ESS) is one of the most popular tools for this purpose. Like most site survey tools, ESS supports both passive and active site surveys. An active survey measures sent packets and received packets. This mode is used to determine metrics such as packet loss and packet delay. A passive survey listens to probes and beacons passively and is useful for creation of coverage and SNR (Signal to Noise Ratio) maps. ESS also supports a hybrid survey mode that simultaneously performs a passive and active survey. We recommend you use the hybrid mode.



These are guidelines for a post-deployment validation survey:

- If you use Ekahau, use Hybrid survey mode. Use Passive or Active mode if you use another tool
- Survey both the 2.4 GHz and 5 GHz bands
- Disable Auto Channel (ACS/DCS)
- Remove all SSIDs from the client excluding the SSID you will survey
- Gather a sufficient number of data points (for example, 1 data point for every 10 to 20 feet)
- Perform the survey with doors closed

Summary of Recommendations for an AP Placement and Channel Plan

This table provides a summary of the recommendations for an AP placement and channel plan.

Recommendations	Notes
Use a predictive site survey application.	The predictive site survey can automate the AP placement and channel capacity planning process.
Consider 1-for-1 AP replacement.	Only implement 1-for-1 replacement if conditions are true as outlined in the One-for-One AP Replacement section of this guide.
SNR should be 25 dB or greater throughout the coverage area.	
Minimum RSSI should be -62 dBm throughout the coverage area.	If designing for 256 QAM rates everywhere the minimum RSSI should be -52 dBm (w/ 80MHz channels).
Clients should see two to three APs (on different channels) at RSSI of -70 dBm or greater.	
Consider deploying one full-time WIPS sensor for every three to five APs.	Depends on security requirements.
Distance between two APs should be approximately 30 to 70 feet.	
Reduce AP transmit power.	Classroom: 5 GHz: 8 to 16 dBm 2.4 GHz: 4 to 10 dBm Auditorium or Lecture Hall: 5 GHz: 5 to 12 dBm 2.4 GHz: 3 to 10 dBm
APs may be ceiling or wall-mounted.	Consider back lobe radiation of antenna when you use a wall mount.

Recommendations	Notes
Disable 2.4 GHz radios on a percentage of APs.	Percentage of APs with disabled 2.4 GHz radios depends on how many unique 5 GHz channels are in use. The more 5 GHz channels in use the greater the % of APs that should have there 2.4Ghz radios disabled.
AP placement and channel plan should use channels to minimize CCI and ACI.	
Stagger APs across floors.	
Consider directional antennas for very high client density deployments.	
For high ceilings (higher than 30 feet / 9.14 meters), high gain (6-9 dB) patch antennas are recommended.	
Adjust AP output power in relation to antenna gain.	
Know the antenna radiation patterns and focus gain towards clients.	
Do not place APs near lighting fixtures or conductive material.	
Do not place APs above ceiling tiles.	
Perform a thorough post - deployment site survey.	

Deployment Use Cases

This section provides solutions for three common use cases in an educational campus environment. Each use case includes simplified AP placement and channel plans.

Use Case 1 – Classroom

A classroom environment can be a challenging use case because of the combination of moderate to high client density, a relatively high per-client throughput requirement, and the close proximity of multiple classrooms. Video-based learning has become more prevalent, and this solution is optimized for a classroom video use case.

Requirements

- 30 client devices active concurrently in each classroom
- Tablets 802.11ac 1x1
- 4 Mbps throughput

Environment

- All DFS channels are available
- Interior walls have moderate attenuation

Channel Capacity Planning

For this use case, there are 30 tablets that are 802.11ac 1x1 active concurrently in each classroom. To support HD video, the throughput requirement for each client is 4 Mbps. In this example, DFS channels are available so we use an 80 MHz channel plan.

This channel capacity estimation is for a single classroom. The proposed solution can be scaled upwards to accommodate the total number of classrooms.

Step 1

Before you begin your calculations, you must know the estimated channel capacity per radio. You can find this information in [Channel Capacity Estimates](#). When you reference the estimated channel capacity tables, an estimated clients per radio density is required. Because the classroom must support 30 concurrently active clients, this use case falls into the moderate density category,

Use Case	Device Type	Number of Active Devices / Density	Application and Client required Bitrate	Channel Capacity	Per Device Airtime / Channel Capacity
Classroom	Tablets 11ac 1x1	30 / Moderate	HD Video (720p) / 4 Mbps	139 Mbps/80 MHz	2.88%

The moderate density table in [Channel Capacity Estimates](#) shows that for 802.11ac 1x1 clients (1 Spatial Stream) with an 80 MHz channel, the estimated throughput capacity is 139 Mbps. To determine the percentage of airtime or channel utilization an individual client requires to meet a per-client throughput requirement, divide the throughput requirement by estimated channel capacity and multiply by 100.

- $(\text{App Bitrate or throughput} / \text{Channel Capacity}) \times 100 = \text{Per Device Airtime}$
- $(4 \text{ Mbps} / 139 \text{ Mbps}) \times 100 = 2.88\%$
- $\text{Per Device Airtime} = 2.88\%$

Step 2

You must now determine the total channels/radios required to deliver the throughput requirement to all clients simultaneously.

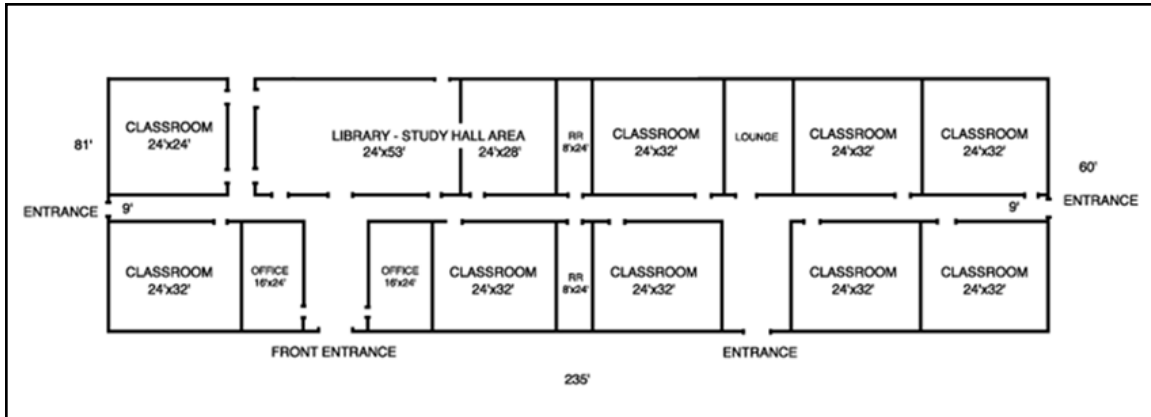
Use Case	Device Type	Number of Active Devices / Density	Per Device Airtime	Total Airtime	Estimated Channels / Radios Required
Classroom	Tablets 11ac 1x1	30 / Moderate	2.88 %	86 %	1

To estimate the total channels/radios required, multiply the per-client airtime required by the total number of clients active concurrently:

- $\text{Number of Active Devices} \times \text{per Device Airtime} = \text{Channels/Radios Required}$
- $30 \text{ Active Devices} \times 2.88\% \text{ per Device Airtime} = 86.3\%$
- $\text{Channels/Radios Required} = 1 \text{ (Rounding up)}$

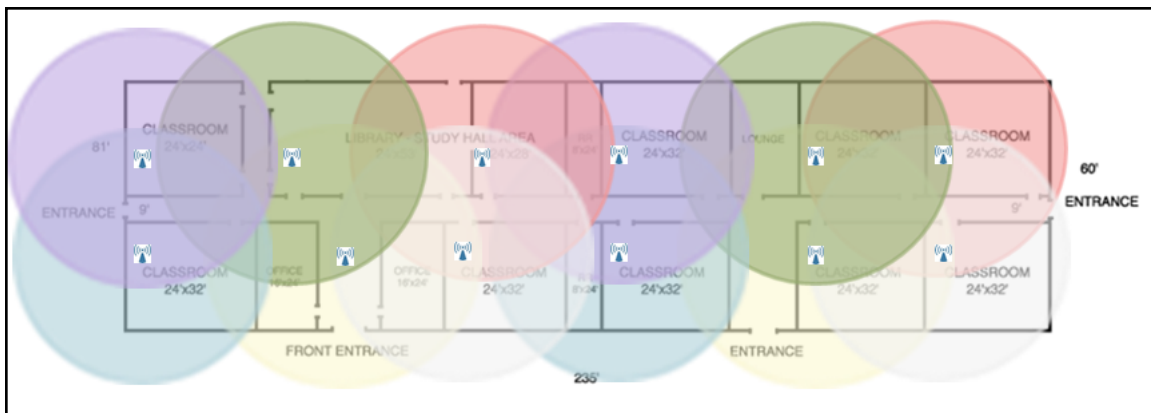
Solution







This image shows the floor plan for a wing of the school building.



5 GHz Plan

This image shows the AP placement and 5 GHz channel plan for a wing of a school building. We recommend you use the AP420 for this use case. There are 12 ceiling-mounted AP420 devices for this wing of the building, each with an active 802.11ac radio (80 MHz).






Color	Channels
	36E
	52E
	100E
	116E
	132E
	149E

2.4 GHz Plan

This image shows the AP placement and 2.4 GHz channel plan for a wing of school building. While there are twelve AP420 devices used for this wing of the building, only seven of them have their 2.4 GHz radios enabled. Five of the 2.4 GHz radios are disabled to reduce the level of CCI in the 2.4 GHz band.



Color	Channels
	1
	6
	11

Use Case 2 – Lecture Hall

It can be a challenge to support a very high number of devices in a relatively confined space. These use cases are common in education environments. For this sample use case, at peak times there can be as many as 200 devices connected to the wireless network simultaneously.

For this use case, the device population is made up of an even mix of 802.11ac 1x1, 2x2 or 3x3 clients. The exact ratio of clients varies from day to day but for planning purposes, we recommend that you plan for 2x2 clients to simplify the process. If there were a larger proportion of 1x1 clients compared to 2x2 and 3x3, you would plan for 1x1 clients. Client fingerprinting capabilities in the current wireless network is the best way to determine a client mix for your use case.

Requirements

- 200 devices active concurrently in the lecture hall
- Mix of 802.11ac devices (1x1, 2x2, and 3x3)
- 3 Mbps throughput requirement

Environment

- All DFS channels excluding 100 are available
- All APs in the lecture hall are within line of sight of each other

Channel Capacity Planning

For this use case, there a mix of 200 802.11ac laptops, tablets, and smart phones that are active concurrently. The per client throughput requirement is 3 Mbps. All DFS channels are available, excluding 100 as the currently installed wireless network has detected radar activity on channel 100. We recommend an 80 MHz channel plan for this use case. If you use auto channel selection, then you must exclude channel 100 from the auto channel candidate list in the radio settings of the Device Template.

Step 1

The tables in [Channel Capacity Estimates](#) help determine the estimated channel capacity. The estimated per radio density for this use case is likely very high because the requirement is to accommodate 200 active clients in a confined area. The use of 2x2 clients in this plan simplifies the design process.

Use Case	Device Type	Number of Active Devices / Density	App or Throughput requirement Bitrate	Channel Capacity	Per Device Airtime / Channel Capacity
Lecture Hall	Design for 11ac 2x2	200 / Very High	3 Mbps	173 Mbps/80 MHz	1.73%

The very high client density table in [Channel Capacity Estimates](#) shows that for 802.11ac 2x2 clients (2 Spatial Streams), with an 80 MHz channel, the estimated throughput capacity is 173 Mbps. To determine the percentage of airtime or channel utilization an individual client requires to meet a per client throughput requirement, divide the throughput requirement by estimated channel capacity and multiply by 100.

- $(\text{App Bitrate or throughput} / \text{Channel Capacity}) \times 100 = \text{Per Device Airtime}$
- $(3 \text{ Mbps} / 173 \text{ Mbps}) \times 100 = 1.73\%$
- $\text{Per Device Airtime} = 1.73\%$

Step 2

You must determine the total channels/radios required to deliver the throughput requirement to all clients simultaneously.

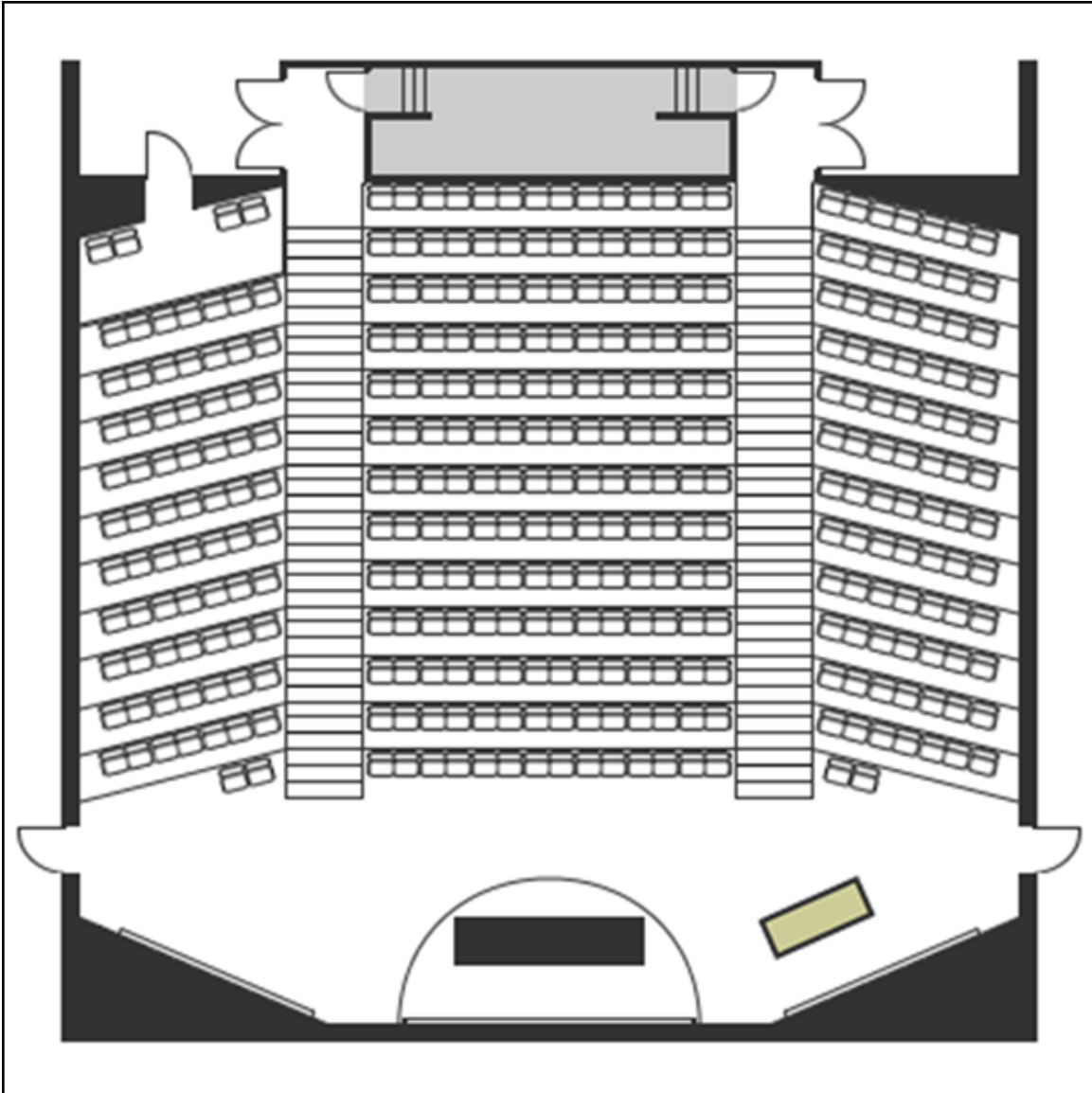
Use Case	Device Type	Number of Active Devices / Density	Per Device Airtime	Total Airtime	Estimated Channels / Radios Required
Lecture Hall	Design for 11ac 2x2	200	1.73%	347%	4

To estimate the total channels/radios required, multiply the per client airtime required by the total number of clients active concurrently.

- $\text{Number of Active Devices} \times \text{per Device Airtime} = \text{Channels/Radios Required}$
- $200 \text{ Active Devices} \times 1.73\% \text{ per Device Airtime} = 347\%$
- $\text{Channels/Radios Required} = 4 \text{ (Rounding up)}$

Solution

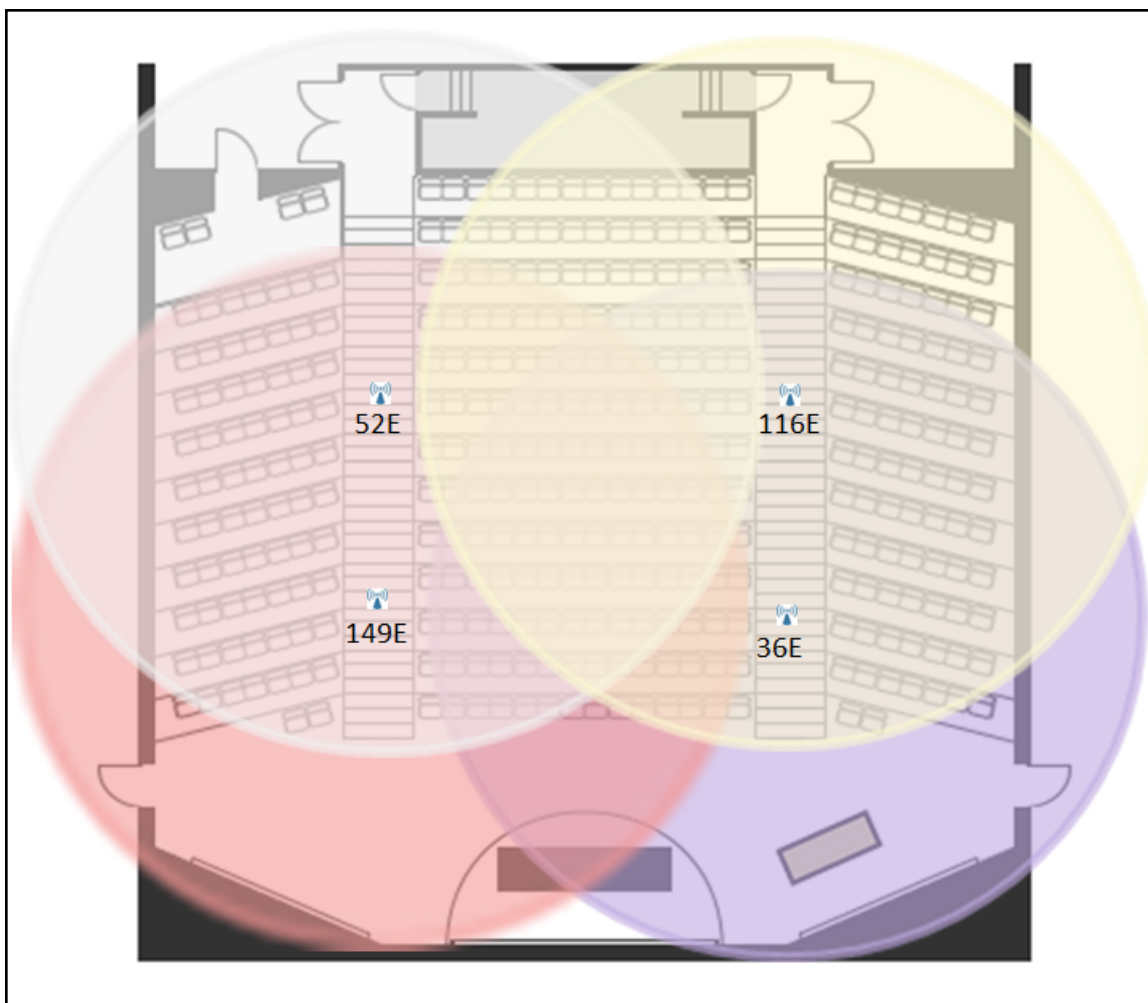
This image shows the lecture hall floor plan.



Auditorium Floor plan

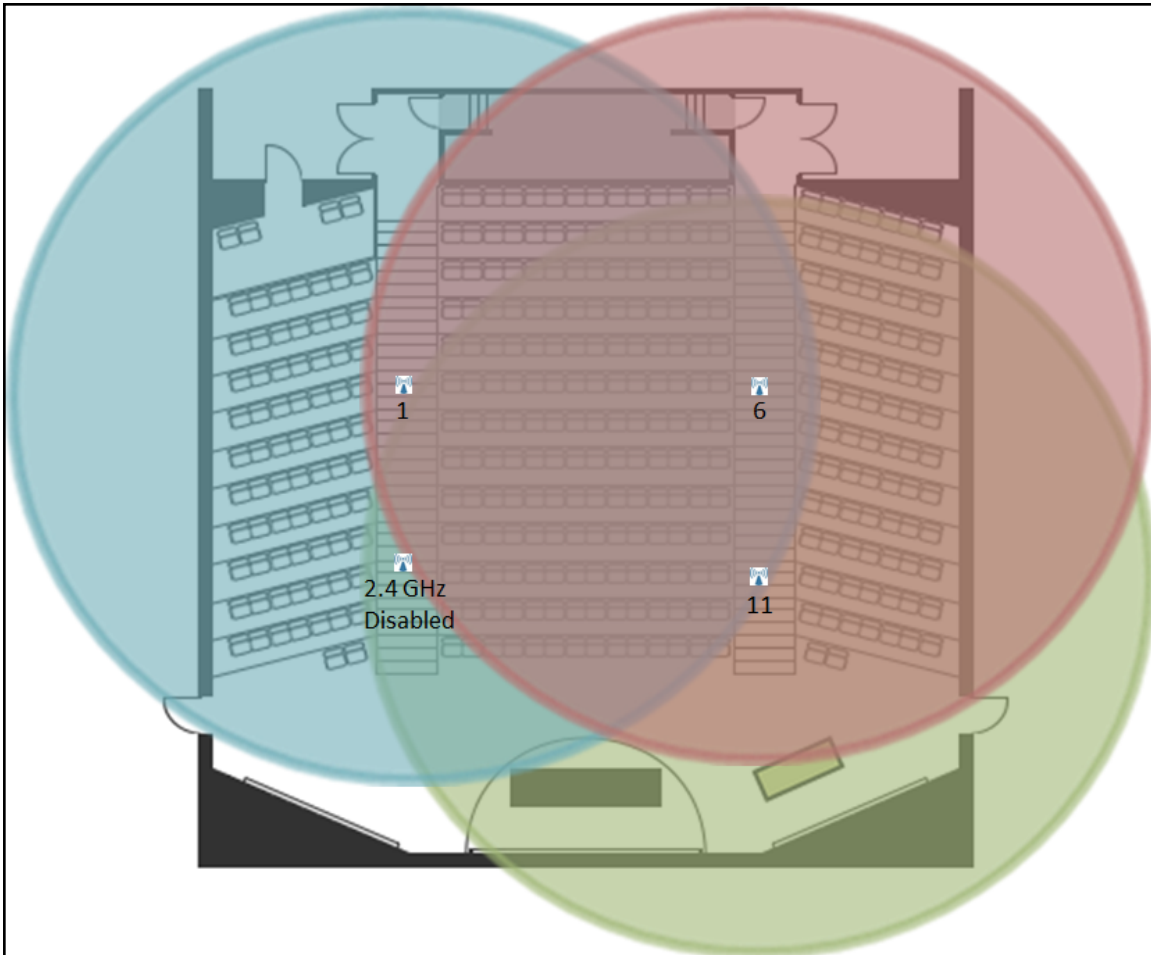
5 GHz Plan

This image shows the AP placement and 5 GHz channel plan for the lecture hall. We recommend you use the AP420 for this use case. A total of four ceiling-mounted AP420 devices are used for the lecture hall, each with an active 802.11ac radio (80 MHz).



2.4 GHz Plan

This image shows the AP placement and 2.4 GHz channel plan for the lecture hall. While there are four AP420 devices used for the lecture hall, only three have their 2.4 GHz radios enabled. One of the 2.4 GHz radios is disabled to reduce the level of co-channel interference (CCI) in the 2.4 GHz band.



Use Case 3 – Dormitories

Students in dorm rooms depend on solid connectivity and performance to do homework, in addition to streaming movies and playing video games. Dorm room walls often have very high levels of RF attenuation. Install APs directly in the dorm rooms for a high signal strength (-62 dBm or greater) throughout the rooms.

Requirements

- 10 devices active concurrently in each dorm room
- Mix of 11n and 11ac devices (1x1, 2x2 and 3x3)
- 5 Mbps throughput requirement

Environment

- DFS channels are not available
- Dorm room walls have very high levels of attenuation

Channel Capacity Planning

For this use case there are 10 devices that are a mix of 802.11n and 802.11ac devices (1x1, 2x2 and 3x3), active concurrently in each dorm room. The requirement is to provide each client with a per client throughput requirement of 5 Mbps. DFS channels are not available so a 40 MHz channel plan is required.

This is a channel capacity estimation for a single dorm room. The proposed solution scales upwards to accommodate the total number of dorm rooms.

Step 1

For this use case the clients per radio density is low. Check the low client density table in [Channel Capacity Estimates](#) to get an estimated throughput capacity. For a mix of 802.11n and 802.11ac clients, we recommend a design for 802.11ac 1x1 or average clients.

Use Case	Device Type	Number of Active Devices/Density	App or Throughput requirement Bitrate	Channel Capacity	Per Device Airtime / Channel Capacity
Dorm Room	Design for 11ac 1x1	10 / Low	5 Mbps	70 Mbps/40 MHz	7.14%

The low client density table in [Channel Capacity Estimates](#) shows for 802.11ac 1x1 clients (1 Spatial Stream) with a 40 MHz channel, the estimated throughput capacity is 70 Mbps. You must determine the percentage of airtime or channel utilization an individual client requires to meet a per client throughput requirement.

- $(\text{App Bitrate or Throughput requirement} / \text{Channel Capacity}) \times 100 = \text{Per Device Airtime}$
- $(5 \text{ Mbps} / 70 \text{ Mbps}) \times 100 = 7.14\%$
- Per Device Airtime = 7.14%

Step 2

You must determine the total channels/radios required to deliver the throughput requirement to all clients simultaneously.

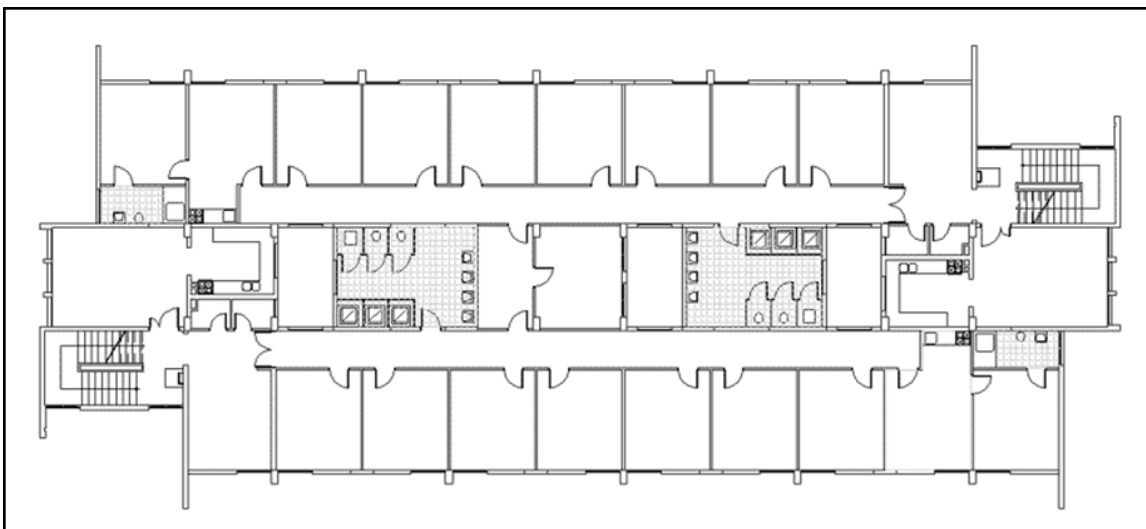
Use Case	Device Type	Number of Active Devices	Per Device Airtime	Total Airtime	Estimated Channels / Radios Required
Dorm Room	Design for 11ac 1x1	10	7.14%	71.4%	1

To estimate the total channels/radios required, multiply the per client airtime required by the total number of clients active concurrently.

- Number of Active Devices x per Device Airtime = Channels/Radios Required
- $10 \text{ Active Devices} \times 7.14\% \text{ per Device Airtime} = 71.4\%$
- Channels/Radios Required = 1 (Rounding up)

Solution

This image shows the floor plan for a wing of the dormitory.



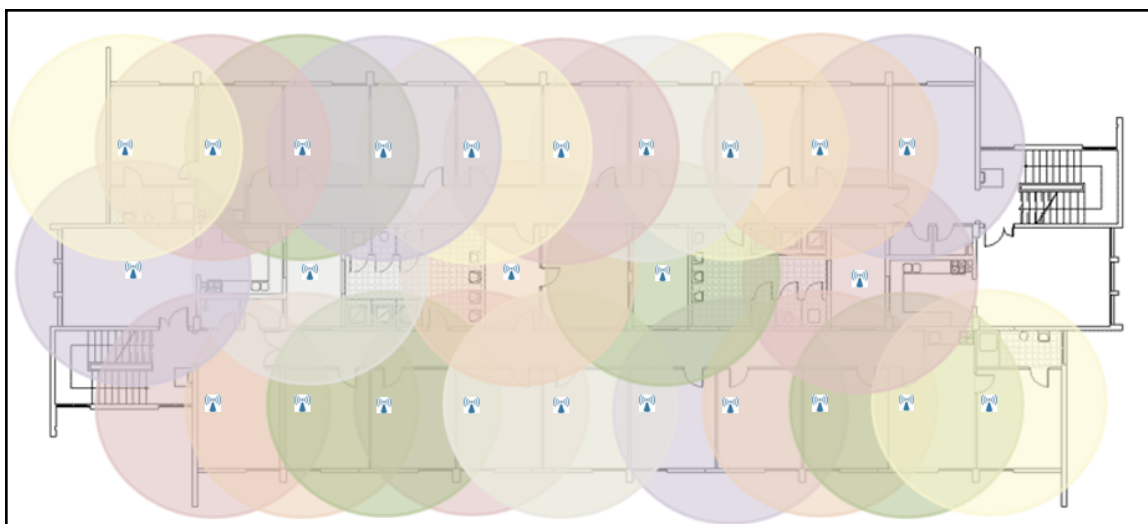
For this solution, you must deploy one AP per room because of the very high attenuation properties of the material used in the wall construction. For dorms with walls that have less attenuation, one AP per two rooms is preferable.







The proposed solution uses a 40 MHz channel. For a one AP per two room plan, you could use an 80 MHz plan to support the 5 Mbps per device throughput requirement. The number of devices per AP would double but so would the approximate throughput capacity of each AP.

We recommend you use an AP125, AP225W, or AP325 for this use case.

5 GHz Plan

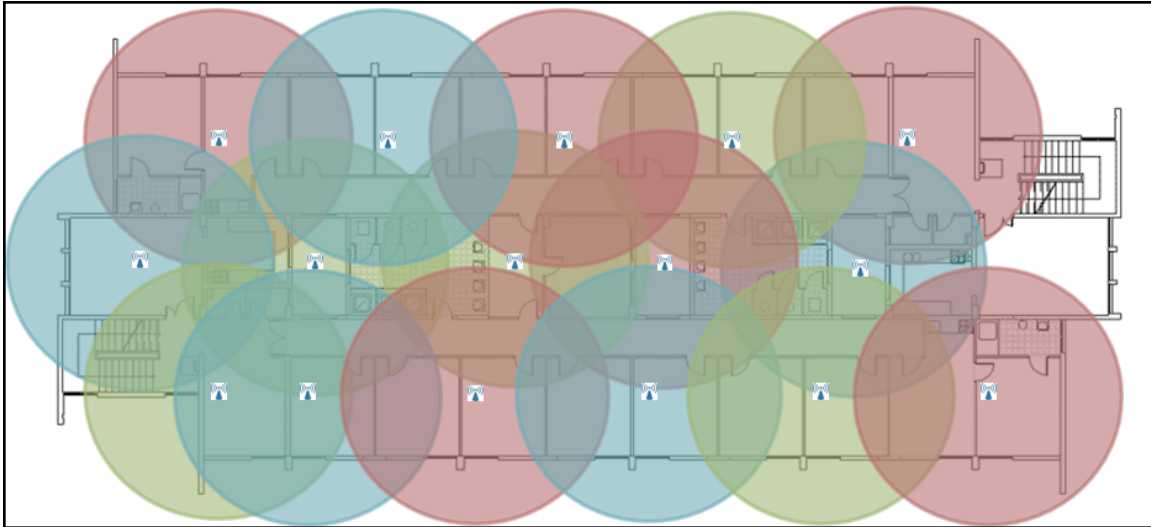
This image shows the AP placement and 5 GHz channel plan for the dormitory with one AP per room. A total of 25 APs are used for the dormitory, each with an active 802.11ac radio (40 MHz).






Color	Channels
	36+
	44+
	100+
	132+
	149+
	157+

2.4 GHz Plan

This image shows the AP placement and 2.4 GHz channel plan for the dormitory. While there are 25 APs used for the dormitory, only 16 of them have their 2.4 GHz radios enabled. 2.4 GHz radios are disabled to reduce the level of co-channel interference (CCI) in the 2.4 GHz band.



Color	Channels
	1
	6
	11

Channel Capacity Estimates

These capacity estimation tables are for reference only. Actual capacity depends on environmental conditions, levels of co-channel interference (CCI) and adjacent channel interference (ACI), client behavior, and quality of wireless network design. You can use predictive survey tools to automate capacity planning. The capacity estimations presented in this section are for a hands-on approach to capacity planning.

These capacity tables only consider 5 GHz capacity. As most wireless LANs also include capacity in the 2.4 GHz band, this results in a built-in capacity buffer provided by the 2.4 GHz band that is typically a small fraction of the capacity in 5 GHz. The size of the 2.4 GHz capacity buffer depends on how clients are distributed across bands and the ratio of 5 GHz spectrum to 2.4 GHz spectrum in use.

Estimated Max Throughput Capacity - 60 % Max Data Rate

1 Client Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	52 Mbps	120 Mbps	260 Mbps	520 Mbps
2 Spatial Streams	104 Mbps	240 Mbps	520 Mbps	1.04 Gbps
3 Spatial Streams	173 Mbps	360 Mbps	798 Mbps	1.40 Gbps
4 Spatial Streams	208 Mbps	480 Mbps	1.04 Gbps	2.08 Gbps

This table is for low-density use cases where there is minimal loss (~ 5%) due to contention and the loss caused by signal strength degradation and rate adaptation are estimated to be 20%.

Estimated Low Density Throughput Capacity - 35 % Max Data Rate

1 - 15 Clients Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	30 Mbps	70 Mbps	151 Mbps	303 Mbps
2 Spatial Streams	61 Mbps	140 Mbps	303 Mbps	607 Mbps
3 Spatial Streams	101 Mbps	210 Mbps	465 Mbps	821 Mbps
4 Spatial Streams	121 Mbps	280 Mbps	607 Mbps	1.21 Gbps

This table is for moderate density use cases where there is moderate loss (~ 8%) due to contention and the loss caused by signal strength degradation and rate adaptation are estimated to be 20%.

Estimated Moderate Density Throughput Capacity - 32 % Max Data Rate				
16 - 30 Clients Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	28 Mbps	64 Mbps	139 Mbps	277 Mbps
2 Spatial Streams	55 Mbps	128 Mbps	277 Mbps	555 Mbps
3 Spatial Streams	92 Mbps	192 Mbps	426 Mbps	750 Mbps
4 Spatial Streams	111 Mbps	256 Mbps	555 Mbps	1.11 Gbps

This table is for high-density use cases where there is high loss (~ 13%) because of contention and the loss caused by signal strength degradation and rate adaptation is estimated to be 20%.

Estimated High Density Throughput Capacity - 27 % Max Data Rate				
31 - 45 Clients Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	23 Mbps	54 Mbps	117 Mbps	234 Mbps
2 Spatial Streams	47 Mbps	108 Mbps	234 Mbps	468 Mbps
3 Spatial Streams	78 Mbps	162 Mbps	359 Mbps	633 Mbps
4 Spatial Streams	94 Mbps	216 Mbps	468 Mbps	938 Mbps

This table is for very high-density use cases where there is very high loss (~20%) because of contention and the loss caused by signal strength degradation and rate adaptation is estimated to be 20%.

Estimated Very High Density Throughput Capacity - 20 % Max Data Rate				
46 - 60 Clients Active	20 MHz	40 MHz	80 MHz	160 MHz
1 Spatial Stream	17 Mbps	40 Mbps	87 Mbps	173 Mbps
2 Spatial Streams	35 Mbps	80 Mbps	173 Mbps	347 Mbps
3 Spatial Streams	58 Mbps	120 Mbps	266 Mbps	469 Mbps
4 Spatial Streams	69 Mbps	160 Mbps	347 Mbps	695 Mbps

