AP 7161
SYSTEM PLANNER

Version	Date	Description
1.0	11.12.2012	Initial

Table of Contents

1 Overview

1.1 Introducing AP 7161

The AP 7161 is a high performance, rugged 802.11n mesh access point that features 300Mbps 2.4 GHz and 5.x GHz radios that support 3x3 MIMO. AP 7161 has been optimized within the Zebra WiNG 5 platform to provide leading capacity, performance and design. The AP7161 is an ideal product for customers who are considering enterprise campus extensions, retail and warehousing applications, together with video surveillance and public safety deployments. At a high-level, the following outlines a brief feature summary for the AP 7161:

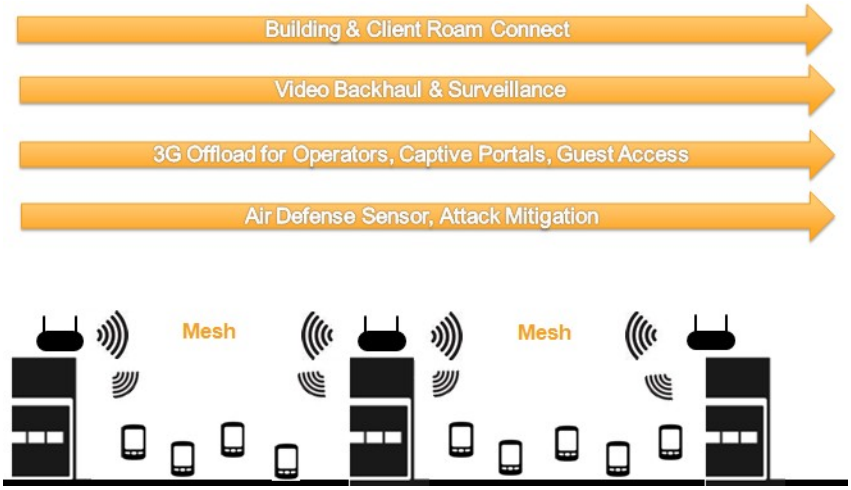
- *Dual-Band Design; 802.11a/b/g/n in the 2.4GHz / 5.XGHz / 4.9Ghz frequency bands*
- *Optional Tri-Radio version which include WIPS sensor radio*
- *20/40 MHz channel width in both 2.4GHz/5Ghz/4.9Ghz (4/9 GHz is 20 MHz only)*
- *True 3x3 MIMO*
- *Frame aggregation (AMSDU/ AMPDU)*
- *Reduced inter-frame spacing*
- *300 Mbps data rates per radio*
- MeshConnex™ Self-*forming and self-healing wide-area wireless mesh routing, providing increased network availability and robustness.*
- *802.11i, WPA2 and WPA; IPSec Encryption*
- *Differentiated services using IP QoS 802.11e.*
- *WiNG 5 configuration management and network monitoring*

NOTE: Wireless Manager will not support the AP7161. Configuration management and network monitoring is provided by the WiNG RFS switch platform or via the Virtual Controller feature.

1.1.1 Use Cases

Before anyone can design a good system, they must understand the wireless and mobility requirements for the target market. The following sections take a closer look at applications in various use cases.

1.1.1.1 Extending Campus, Education and Telecoms / Media, Applications Outdoors



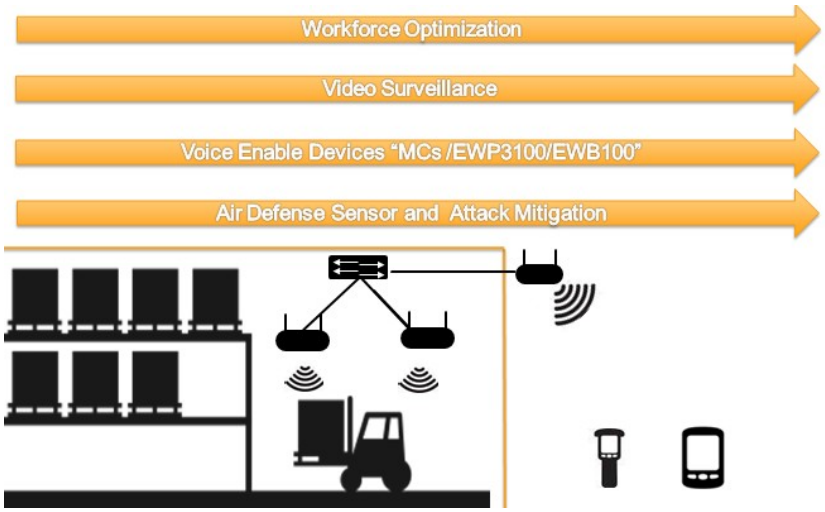
The ability to extend a wireless network to the outdoors has become a very common application within enterprises, education and campuses. The ability to roam and maintain connection between buildings with applications is an ideal use case for AP 7161.

In addition the placement of an outdoor AP 7161, it can be used as an asset to drive applications to the outdoors. Each AP 7161 has two gigabit Ethernet ports and the power of MeshConnex™ that can enable cameras at location previously not served for safety and surveillance, and the transport of video via wireless backhaul for low site applications.

With increasing usage of smart phones in the enterprise comes a significant increase in data usage over cellular networks. This increase in data traffic is clogging 3G cellular networks and degrading the user experience. The AP 7161 can help enterprises and carriers alike offload this traffic to a Wi-Fi network. Together with guest access and captive portal technologies the AP7161 provides safe and secure data transactions.

Lastly when we extended wireless coverage into outdoor scenarios we must always be aware of threats and attacks to corporate and public networks alike. The AP 7161 is taking a new style of defense mechanism with Airdefense technology to mitigate attacks and wireless intrusion to outdoor networks, with an onboard WIPS sensor.

1.1.1.2 Extending Transportation, Logistics, Warehousing and Airport Operations, Applications Outdoors

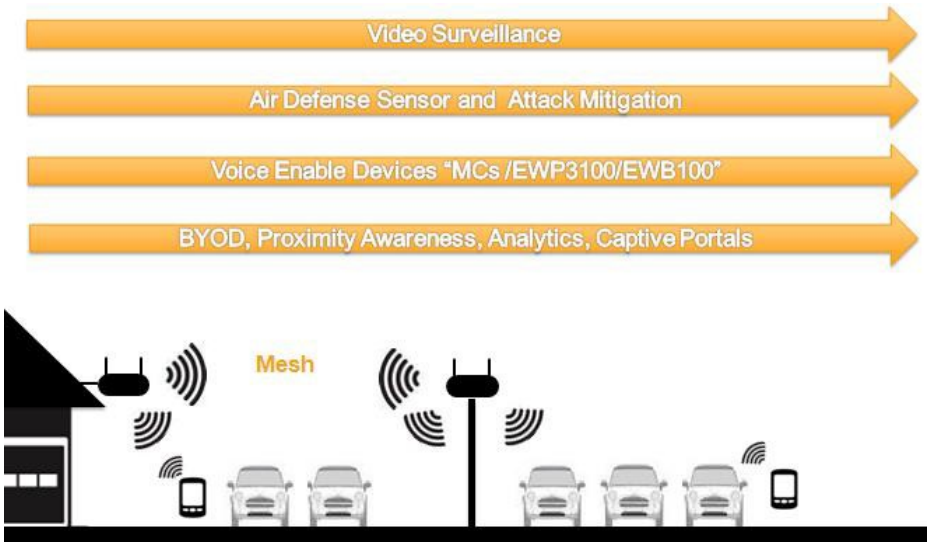


Workforce optimization matched with seamless indoor and outdoor coverage is enabling rugged terminals and handhelds, such and Zebra MC Terminals and the ET1 to be used in extended coverage to terminal docks, lot yards and airport operations. The nature of the WiNG architecture allows for management to be both centralized and or decentralized giving greater flexibility deployment strategies and upgrades as required.

As example within an airport operation which is by nature a multi tenant environment the use of a comprehensive VLAN architecture allows multiple secure entities(airlines, airport management, handlers and the public to co-exist on a single AP 7161 infrastructure, with multiple form factor devices reaching indoors to outdoors. There is also a need in this example for flexible low site video surveillance, and the ability for clients to securely receive video applications remotely and in real time all enabled by AP 7161. There is also a case for extending voice to the

outdoor network and having a client/VoIP device roam seamless between the indoor and outdoor network. Supporting voice and data services using enhanced QOS is possible for this operation using AP 7161. The need to secure perimeters of facilities has become a must, and the use of the onboard sensor technology WIPS enables operations to understand who is using a device in an operation, and decide whether they pose a threat or not. The WIPS sensor is also being used in an outdoor environment to locate devices and infrastructure that has been deployed without authorization allowing enterprises to mitigate these forms of rogue or unauthorized devices.

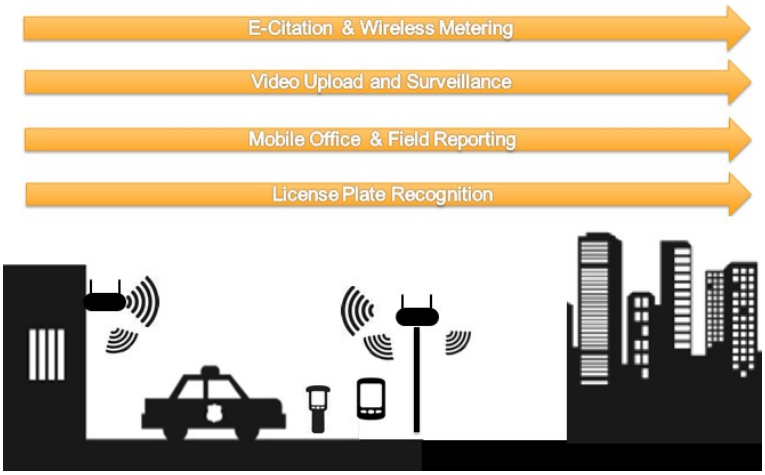
1.1.1.3 Extending Retail, Applications Outdoors



Retail markets are looking to expand wireless connectivity beyond the store walls to drive applications to the perimeters and parking lots in various store locations. As in the example above this retailer is looking to use the location of the AP 7161 devices to provide coverage access where it may offer BYOD (bring your own device) services and captive portals for hotspot access, or even enable its own employees to have connectivity outdoors. In the same fashion those analytics and proximity awareness applications can be deployed in the outdoors to look at consumer device traffic patterns and usage.

Coupled to the location of the access point this sample retail customer is using the mesh backhaul to bridge wireless security and surveillance cameras from the AP 7161 location providing asset protection, and consumer safety. Having an outdoor wireless mesh system is also going to allow VoIP wireless handsets to be deployed for concierge applications and provide security to protect the network and users from rogue devices and attacks to users and employees alike.

1.1.1.4 Public Safety



For many years Public Safety has embraced the benefits of secure wireless data and mobility applications. With products such as the AP 7161 these organizations and departments can bring new applications to field officers and operations. For example taking an outdoor connection to the parking lots of a police station, or a hotspot within the urban environment using 4.9GHz, allows officers and patrols to field report real time, or allow a DVR offload of video records from vehicles in downtimes, increasing productivity and efficiency savings.

Public safety departments are deploying single outdoor wireless access networks across urban environments, allowing multiple departments and law enforcement agencies to deliver a variety of applications, such as parking enforcement applications, wireless metering, and video surveillance.

1.1.1.5 Multi-Use City Wide

Cities are focusing outdoor networks on dedicated hotspot applications, allowing multiple agency applications to have wireless access reducing overhead and cost structures in city departments for:

- *Smart Phones*
- *Smart Meter Reading*
- *Water Meters*
- *Traffic Control*
- *Smart Parking*
- *Remote Building Management*

1.2 802.11n Technology Introduction

802.11n provides many enhancements that improve 802.11 wireless network performance. 802.11n introduces enhancements to the 802.11 Media Access Control (MAC) and Physical (PHY) layers that produce higher throughputs and increased range over legacy 802.11 a/b/g systems. In addition to these performance enhancements 802.11n remains backward compatible with these legacy systems. This section will explore these enhancements.

1.2.1 MIMO

MIMO or **Multiple Input Multiple Output** is the technique of using multiple transmit and receive antennas. Most legacy 802.11a/b/g systems are SISO or Single Input Single Output systems. In a SISO system the transmitter and receiver utilize a single antenna.

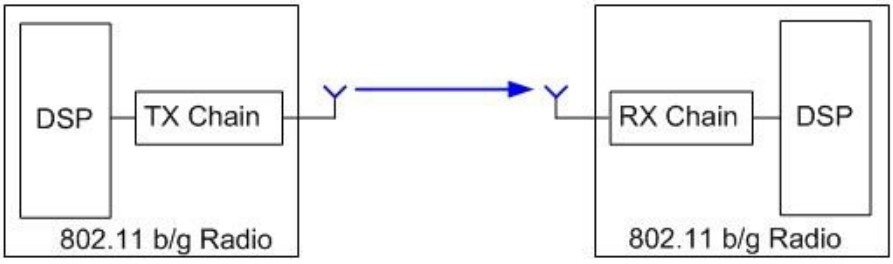


Figure 1-1

MIMO systems can come in different configurations. For example a 2×2 MIMO configuration would contain 2 transmit and 2 receive antennas. A 3×3 MIMO configuration would contain 3 transmit and 3 receive antennas. Configurations are often expressed by N×M where N is the number of transmitting antennas and M is the number of receiving antennas producing a total of N×M paths.

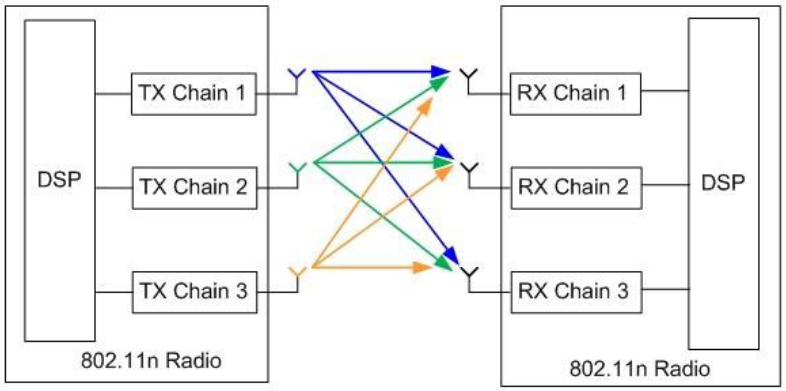


Figure 1-2

MIMO exploits radio multipath. Multipath results when signals reflect off of objects and take different paths between the transmitter and receiver. Signals can arrive at the receiver delayed in time or phase shifted. With first generation SISO radio systems multipath can result in constructive and destructive interference. MIMO takes advantage of multipath with a technique called spatial multiplexing.

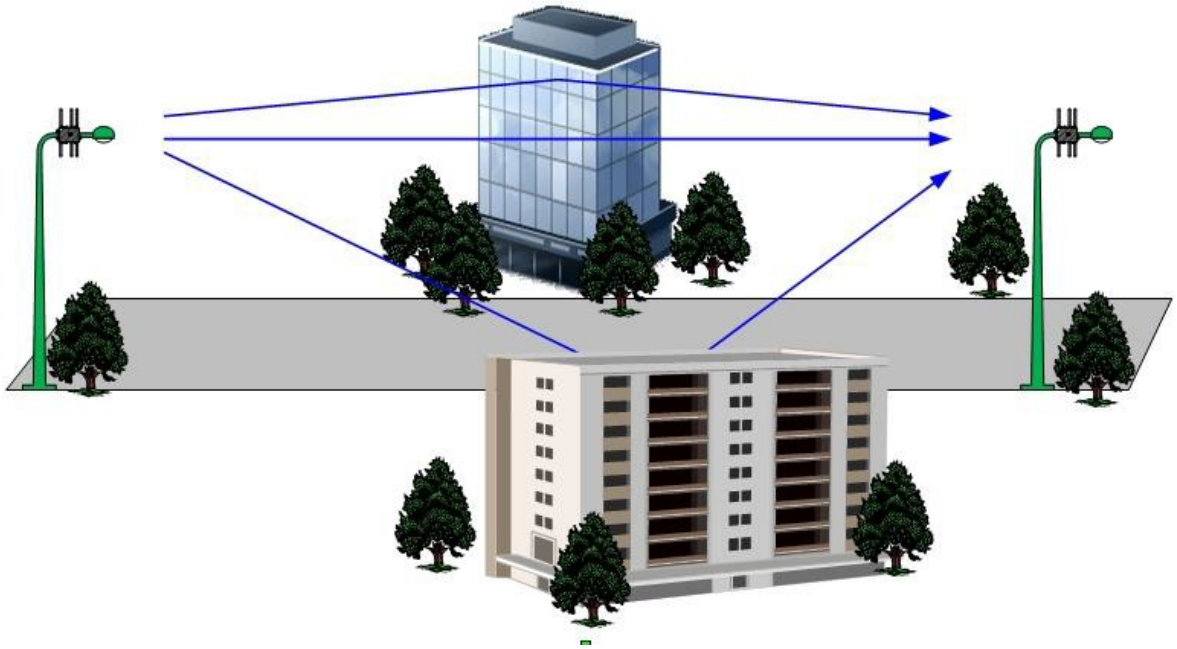


Figure 1-3

1.2.2 Spatial Multiplexing

Spatial multiplexing divides the incoming signal into multiple streams. These streams are transmitted through different antennas. Using multipath these streams propagate along different paths from the transmitter to the receiver. Using advance signal processing techniques the receiver will combine these individual streams back into the original data stream. In a 2×2 MIMO systems using 2 spatial streams the data rate is effectively doubled.

802.11n specifies a minimum of 2 spatial streams and a maximum of 4. MIMO nomenclature is often expanded to include the number of supported streams i.e. N×M:S where S is equal to the number of streams. For example, a 3×3:2 can transmit and receive 2 data streams on its 3 antennas

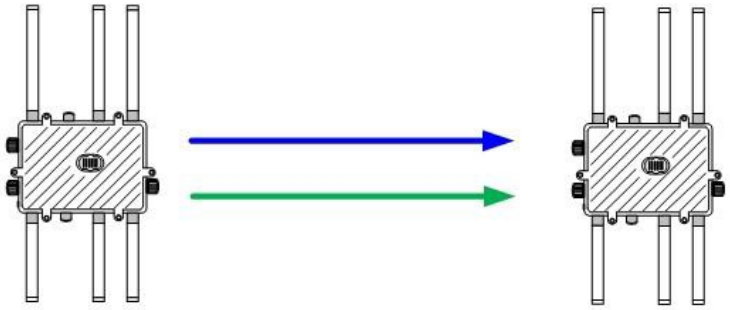


Figure 1-4

1.2.3 MRC

MRC is a receive-side MIMO technique that takes RF signals from multiple receive antennas and combines them within the radio to effectively boost the signal strength. This MIMO technique is fully compatible with 802.11a/b/g devices and significantly improves receiver sensitivity and overall gain for the access point radio, especially in multipath environments.

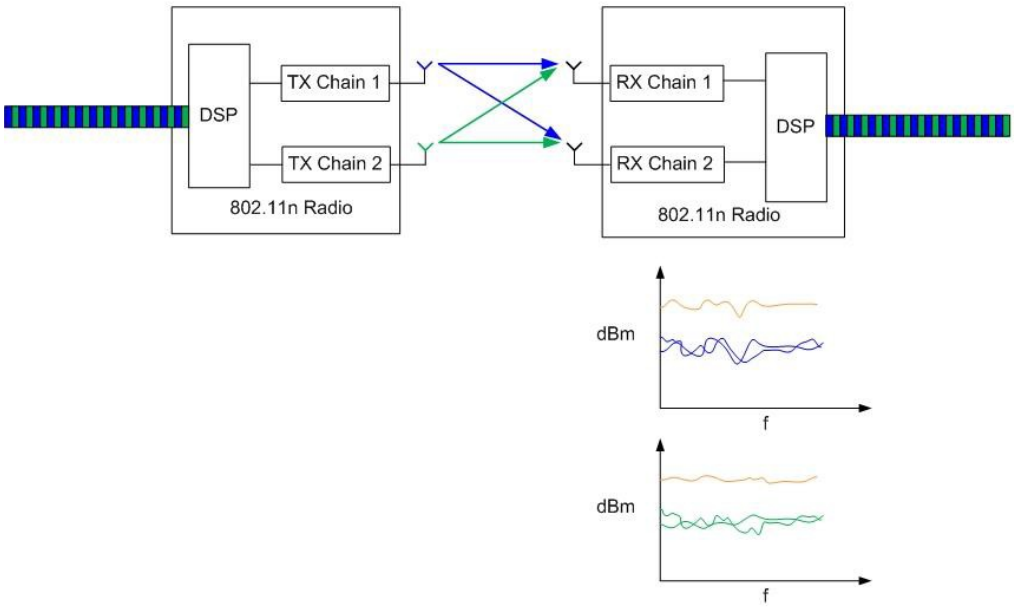


Figure 1-5

1.2.4 Aggregation Techniques

Every 802.11 wireless frame requires a positive Acknowledgement or ACK (the exception being broadcast frames which do not use ACKs and therefore do not get aggregated). This requirement of transmitting an ACK for each control and data frame significantly reduces system performance. 802.11 also requires devices to use a random back off period after each frame before gaining access to the wireless medium to transmit the next frame. There are several key enhancements in 802.11n that improve upon these limitations.

1.2.4.1 MSDU Aggregation

The term MSDU (MAC Service Data Unit) refers to the payload that is carried by the 802.11 MAC layer frame. An MSDU typically consists of an LLC header, IP header and the IP packet payload from layers 4-7. When Mobile Units (MUs) communicate with different hosts in a network they still send all the 802.11 frames to the access point. Access point receives the 802.11 frames and forwards them to appropriate destinations. This may involve adding an 802.3 header if the destination is a wired host or a new 802.11 header if the destination is an 802.11 wireless host. The MSDU aggregation technique exploits this behavior and allows for a mechanism to aggregate multiple payloads in a single 802.11 frame. Since the MU has a single security association with the access point, this large 802.11 frame incurs the overhead of encryption (and decryption at the receiver) only once. This improvement is more pronounced for small size frames. Since an A-MSDU frame is transmitted as a single 802.11 frame, receiver can acknowledge by sending a single ACK frame. There is also a significant increase in the maximum frame payload which reduces the acknowledgement overhead associated with 802.11 communications and improves overall throughput. The maximum A-MSDU size allowed by 802.11n is 8192 bytes. The disadvantage of aggregating A-MSDU is that each frame is only protected by a single checksum and an error in receiving an A-MSDU transmission incurs the overhead of having to retransmit the entire A-MSDU again.

1.2.4.2 MPDU Aggregation with Block ACKs

MPDU (MAC Protocol Data Unit) aggregation gathers 802.11 frames, which each already have an 802.11 header for the same destination and transmits them as a single frame. Since this process involves transmitting multiple 802.11 frames as a single “grouped” frame, each frame requires its own ACK; however, instead of transmitting each ACK individually, 802.11n introduces a Block ACK frame which compiles all the individual acknowledgements into a single frame which gets transmitted from the receiver to the sender. The Block ACK frame is essentially a bitmap, or matrix of which frames are being acknowledged. One of the disadvantages of MPDU aggregation is that each 802.11 frame needs to be encrypted separately, adding encryption overhead. On the other hand, MPDU aggregation allows for the selective retransmission of those frames not acknowledged within the Block ACK. This can be very useful in environments which have a high number of collision or transmission errors. The maximum A-MPDU size allowed by 802.11n is 64K bytes.

1.2.5 Reduced Interframe Spacing (RIFS)

Normal 802.11 transmitters are required to implement a random back off between transmissions. DCF *(Distributed Coordinated Function)* is a contention based service widely implemented in infrastructure networks that defines the back off period for devices. The interframe spacing in DCF is referred to *DCF Interframe Spacing* (DIFS). DIFS is the minimum idle time for transmissions if the medium is idle for longer than the DIFS interval. Wi-Fi Multimedia (WMM) based QoS allows frame bursting for certain devices without requiring a random back off. These WMM devices typically separate their ACK receipt and subsequent transmissions with a shorter interframe spacing,

referred to as *Short Interframe Spacing* (SIFS). 802.11n introduces an even shorter interframe spacing called *Reduced Interframe Spacing* (RIFS).

1.2.6 Short Guard Interval

The guard interval is the space between symbols (characters) being transmitted. This is often confused with the space between packets, which is the interframe space (IFS). The guard interval is there to eliminate inter-symbol interference, which is referred to as ISI. In 802.11n the guard interval can be reduced to 400ns or half of what legacy 802.11 systems use. Shortening the guard interval increases the symbol rate thus increasing performance. However, in a high interference environment Short Guard Interval can result in a higher error rate and reduce performance.

1.2.7 Channel Size

20 MHz Channel Size

Legacy 802.11 a/b/g systems utilize a 20 MHz channel sliced into 48 data carrying subcarriers. 802.11n increases 20 MHz channel data carrying subcarriers from 48 to 52 increasing the maximum data rate to 65 Mbps (single stream). If short guard interval is used in a 20 MHz channel this rate increases to 72 Mbps. For 2 transmitters (2 spatial streams) using a 20 MHz channel the maximum data rate is increased to 65 + 65 = 130 Mbps or 144 Mbps if short guard interval is used.

40 MHz Channel Size

802.11n also includes the option of using a 40 MHz channel that effectively doubles system performance. When using a 40 MHz channel the amount of data carrying subcarriers is increased to 108. This provides a maximum data rate of 135 Mbps (single stream). Using this configuration along with short guard interval the maximum data rate is increased to 150 Mbps. Using 2 spatial streams with a 40 MHz channel the maximum data rate is 135 + 135 = 270 Mbps. Using this configuration along with short guard interval the maximum data rate is increased to 300 Mbps.

One Spatial Steam (MCS 0-7)				Two Spatial Steams (MCS 8-15)		
802.11 a/g Rates	802.11n Mandatory Rates 20 MHz Channel	802.11n Mandatory Rates 40 MHz Channel	Short Guard Interval Enabled	2 Spatial Streams	802.11n Mandatory Rates 40 MHz Channel	Short Guard Interval Enabled
6	6.5	13.5	15	13	27	30
9	13	27	30	26	54	60
12	19.5	40.5	45	39	81	90
18	26	54	60	52	108	120
24	39	81	90	78	162	180
36	52	108	120	104	216	240
48	58.5	121.5	135	117	243	270
54	65	135	150	130	270	300

Figure 1-6

1.3 Product Details

1.3.1 Latest Firmware and Product Documentation

The latest software versions and releases notes for AP 7161 can be found at this location

http://support.symbol.com

1.3.2 Existing Legacy Mesh Customers

Please note the following if you are an existing mesh customer using Duo 4300 or AP7181:

- Compatibility for MWAN 4300 Series and MWAN AP 7181 Series product was introduced in WiNG 5.2.2
- AP-7161 WiNG 5.2.2 was tested with DUO v9.4.16 and AP7181 v3.2.2.0-14MR, v3.2.1.1-20MR, v3.2.1.0-120MR.
- AP7181 is now supported in WiNG 5.4.0

When deploying the AP7161 with legacy mesh products please refer to the MCX How to Guide.

1.3.3 Physical Specifications

1.3.3.1 Chassis Dimensions / Weight

The AP7161 main chassis is approximately 28.1 cm x 21.8 cm x 9.4 cm and has a weight of 6.4 lbs / 2.9Kg. This weight is without antennas or a mounting bracket.

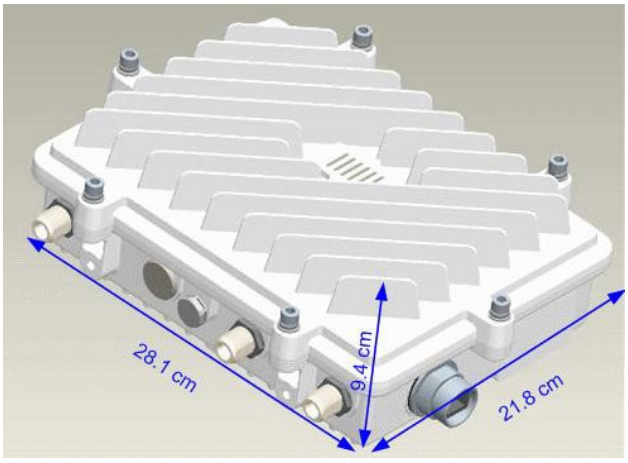


Figure 1-7

1.3.3.2 Environmental

- Operating Temperature -40 to +70 Degrees Celsius
- Storage Temperature -40 to +85 Degrees Celsius
- Operating Humidity 5-95%
- Operating Altitude 8000 Feet
- Storage Altitude 30,000 Feet
- Electrostatic Discharge EN61000-4-2. Air +/-15kV, Contact +/-8kV
- Enclosure Outdoor IP67 rated, corrosion resistant enclosure ASTM
- B117 Salt, Fog, And Rust resistance
- Wind Ratings 150 mph * (unit bracket measurement)
- Operational Shock IEC60721-3-4, Class 4M3, MIL STD 810F
- Operational Vibration IEC60721-3-4, Class 4M3

1.3.4 AP7161 Ordering Overview

The AP 7161 product line comprises of the following categories:

- Product Kits
- Mounting Kits
- Antenna (s)
- POE Accessories

Each Kit AP-7161-66xxx-xx will ship with the following standard items:

- 1 x Waterproof Ethernet Adaptor
- 1 x Installation Guide (with mounting instructions)

You must order the following separately:

- Mounting Kit(s)
- Antenna (s)
- POE Accessories
- RFS Controller if required

Further information can be obtained from the Zebra AP 7161 Ordering Guide.

1.3.4.1 AP-7161-66040-US (Dual Band 2.4 GHz / 4.9 GHz / 5.8 GHz)

This AP7161 SKU is for use in North America and Puerto Rico. When ordering you must also select your antenna options, PoE options, and mounting options. Note that AP-PSBIAS-7161-US is for North America only and has a molded three pin plug to the AC power lead.
Below is an example of what may be ordered to support a single AP. Accessory options may differ based on antenna and deployment choices:

Qty	Part Number	Description
1	AP-7161-66040-US	AP 7161 outdoor 802.11N AP US

3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")
1	AP-PSBIAS-7161-US	IP66 802.3at gigabit Ethernet power injector 100-240VAC US
1	KT-153143-01	AP 7161 outdoor PoE mount kit
1	KT-147407-01	AP 7161 mounting hardware kit - 3 pieces
1	KT-150173-01	AP 7161 12 inch extension arm for mounting kit

1.3.4.2 AP-7161-66040-WR (Dual Band 2.4 GHz / 5.x GHz)

This AP7161 unit is for all other countries not within the US SKU. Note Canada customers should order this part specifically. When ordering you must also select your antenna options, PoE options, and mounting options. Please note that the chassis and PoE injector are different SKUs than the North American version. The difference here is that to comply with international cabling requirements, the AP-PSBIAS-7161-WW is a flying leads cable and not a molded plug.

Below is an example of what may be ordered to support a single AP. Accessory options may differ based on antenna and deployment choices:

Qty:	**Part Number**	**Description**
1	AP-7161-66040-WR	AP 7161 outdoor 802.11N AP International
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")
1	AP-PSBIAS-7161-WW	IP66 802.3at gigabit Ethernet power injector 100-240VAC International
1	KT-153143-01	AP 7161 outdoor PoE mount kit
1	KT-147407-01	AP 7161 mounting hardware kit - 3 pieces
1	KT-150173-01	AP 7161 12 inch extension arm for mounting kit

1.3.4.3 AP-7161-66S40-US (Dual Band 2.4 GHz / 5.8 GHz with WIPS Sensor)

This AP7161 SKU is for use in North America and Puerto Rico. This is a dual band unit that also contains a WIPS sensor radio. When ordering you must also select your antenna options, PoE options, and mounting options. Please make sure you order the correct WIPS specified antenna (ML-2452-HPAG5A8-01). Note that AP-PSBIAS-7161-US is for North America only and has a molded three pin plug to the AC power lead.

Below is an example of what may be ordered to support a single AP. Accessory options may differ based on antenna and deployment choices:

Qty	**Part Number**	**Description**
1	AP-7161-66S40-US	AP 7161 outdoor 802.11N AP with sensor US
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")
2	ML-2452-HPAG5A8-01	Outdoor, dipole, 4.5dBi/7.5dBi, N-Male, multiband
1	AP-PSBIAS-7161-US	IP66 802.3at gigabit Ethernet power injector 100-240VAC US
1	KT-153143-01	AP 7161 outdoor PoE mount kit
1	KT-147407-01	AP 7161 mounting hardware kit - 3 pieces
1	KT-150173-01	AP 7161 12 inch extension arm for mounting kit

1.3.4.4 AP-7161-66S40-WR (Dual Band 2.4 GHz / 5.x GHz with WIPS Sensor)

This AP7161 unit is for all other countries not within the US SKU. Note Canada customers should order this part specifically. This is a dual band unit that also contains a WIPS sensor radio. When ordering you must also select your antenna options, PoE options, and mounting options. Please make sure you order the correct WIPS specified antenna (ML-2452-HPAG5A8-01). To comply with international cabling requirements the AP-PSBIAS-7161-WW is a flying leads cable and not a molded plug.
Below is an example of what may be ordered to support a single AP. Accessory options may differ based on antenna and deployment choices:

Qty	Part Number	Description
1	AP-7161-66S40-WR	AP 7161 outdoor 802.11N AP with sensor International
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")
2	ML-2452-HPAG5A8-01	Outdoor, dipole, 4.5dBi/7.5dBi, N-Male, multiband
1	AP-PSBIAS-7161-WW	IP66 802.3at gigabit Ethernet power injector 100-240VAC International
1	KT-153143-01	AP 7161 outdoor PoE mount kit
1	KT-147407-01	AP 7161 mounting hardware kit - 3 pieces
1	KT-150173-01	AP 7161 12 inch extension arm for mounting kit

1.3.5 AP 7161 Power Options

The AP7161 is powered via a PoE capable switch or external outdoor rated PoE injector. PoE power must be provided on the GE1 Ethernet interface.

- Operating Voltage - 36-57 VDC
- Operating Current - Not to exceed 750mA @ 48VDC

There are two orderable PoE Outdoor Rated options for powering the AP7161:

Countries in North America
AP-PSBIAS-7161-US IP66 802.3at gigabit Ethernet power injector 100-240VAC US

All Other Countries
AP-PSBIAS-7161-WW IP66 802.3at gigabit Ethernet power injector 100-240VAC International

There is also an orderable mounting kit that can be used for either PoE option:
KT-153143-01 AP 7161 outdoor PoE mount kit

1.3.6 Antenna Options

Available antenna options for AP 7161 are as follows;

2.4 GHz Antennas

ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9in)
ML-2499-HPA8-01	Outdoor, dipole, 8dBi, N-Male, 2.4GHz (19.5in)
RAN4054A	Downtilt, 8dBI, N-Male, 2.4 GHz (21in)

5 GHz Antennas

ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6.75in)
ML-5299-HPA10-01	Outdoor, dipole, 10dBi, N-Male, 4.9-5GHz (19.5in)

4.9 GHz / 5 GHz Antennas

ML-5299-FHPA6-01R	Indoor / Outdoor; Type: Dipole; Gain: 8.0 dBi; Beam Width: E-Plane: 16 degrees, H-Plane: 360 degrees; Connector: N Male; Frequency: 4900-5875MHz
ML-5299-HPA10-01	Outdoor, dipole, 10dBi, N-Male, 4.9-5 GHz (19.5in)

Dual Banded Antennas (used for sensor radio)

ML-2452-HPAG5A8-01 Outdoor, dipole, 4.5dBi/7.5dBi, N-Male, multiband 4.5dBi @2.4GHz, 5.5dBi @ 4.9GHz, 7.5dBi @ 5GHz (11in)

NOTE: For increased 2.4 GHz coverage in dense urban environments consider using 2.4 GHz downtilt antennas on the 2.4 GHz radios such as: **RAN4054A -** Downtilt, 8dBI, N-Male, 2.4 GHz (21in)

Example:

A typical configuration for a single **AP-7161-66040-US (Dual Band 2.4 GHz / 5.8 GHz)** might include:

Qty	SKU	Description
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")

Example:

A typical configuration for a single **AP-7161-66040-WR (Dual Band 2.4 GHz / 5.x GHz)** for use in European countries might include:

Qty	SKU	Description
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA10-01	Outdoor, dipole, 10dBi, N-Male, 5GHz (19.5in)

The follow three radio AP7161 SKUs have (3) N-Type Female antenna ports for 2.4 GHz, (3) N-Type Female antenna ports for 5.x GHz, and (2) N-Type Female antenna ports for the WIPS radio.

AP-7161-66S40-US (AP 7161 outdoor 802.11N AP with sensor US)
AP-7161-66S40-WR (AP 7161 outdoor 802.11N AP with sensor International)

Example:

A typical configuration for a single **AP-7161-66S40-US (Dual Band 2.4 GHz / 5.8 GHz)** might include:

Qty	SKU	Description
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA5-01	Outdoor, dipole, 5dBi, N-Male, 5GHz (6")
2	ML-2452-HPAG5A8-01	Outdoor, dipole, 4.5dBi/7.5dBi, N-Male, multiband (11in)

Example:
A typical configuration for a single **AP-7161-6604S-WR (Dual Band 2.4 GHz / 5.x GHz)** for use in European countries might include:

Qty	SKU	Description
3	ML-2499-HPA4-01	Outdoor, dipole, 4dBi, N-Male, 2.4GHz (9")
3	ML-5299-HPA10-01	Outdoor, dipole, 10dBi, N-Male, 5GHz (19.5in)
2	ML-2452-HPAG5A8-01	Outdoor, dipole, 4.5dBi/7.5dBi, N-Male, multiband (11in)

1.3.7 Mounting Hardware

The Universal Mounting bracket (KT-147407-01) can be adjusted to rotate (plus or minus 15 degrees) and tilt (up to 45 degrees) during installation to orient the unit for optimum positioning. Mounting instructions are include in the Product Installation Guide.

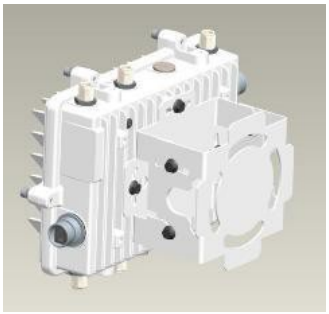


Figure 1-8

When mounting an AP 7161 on poles more than six inches in diameter, a minimum standoff distance of twelve inches is required to avoid interference with the antennas. The 12in extension bracket (KT-150173-01) can be used in combination with the standard mounting bracket when required.

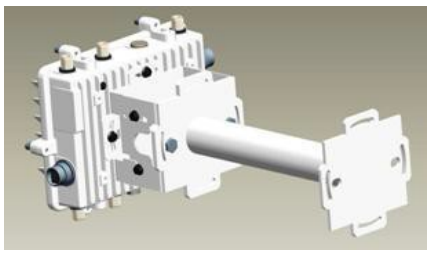


Figure 1-9

NOTE: Please refer to the Product Installation Guide for complete details on device installation

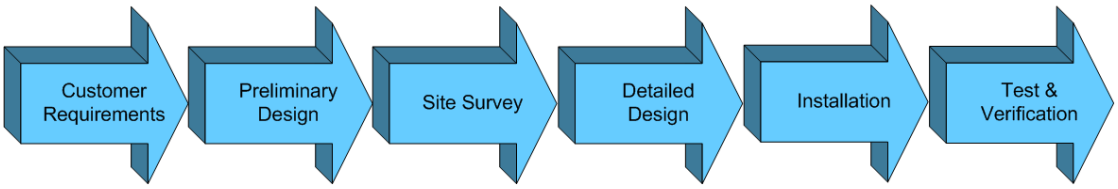
1.3.8 External Ethernet / Console

The AP7161 has (2) Gigabit Ethernet ports and (1) RJ-45 Console port. GE1 is the designated PoE port. Power must be provided to GE1 by either a PoE cable switch or external PoE injector. GE2 can be used to connect an external device such as a surveillance camera. The console port utilizes a standard RJ-45 rollover cable with the following port settings:

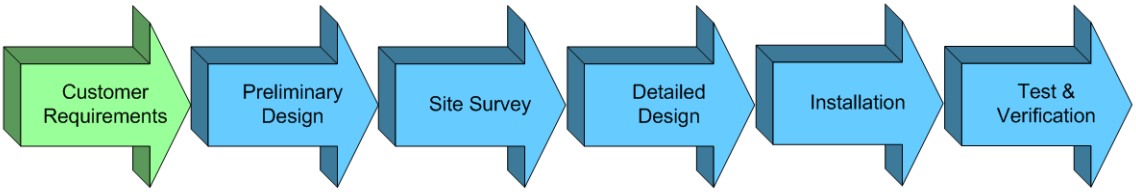
Baud Rate	- 19200
Data	- 8 bit
Parity	- None
Stop	- 1
Flow Control	- None

2 Network Design and Planning

At first, planning a new outdoor wireless project may seem like a very difficult process. Where does one begin? It helps to first break down the process into manageable steps. In the following section we will review a simple methodology for planning and designing an outdoor wireless network using the AP7161.



2.1 Customer Requirements



Defining customer requirements at the beginning of a project is the key to deploying a solution that meets the needs of a customer and their users. It is difficult and costly to re-engineer a network once it is installed. Requirements provide a foundation for the wireless design, where technology selection is a key aspect which defines how the solution will work, and what wireless components are necessary.

2.2 The Customer Use Case

Prior to designing and planning a network is to clearly understand what the customer is trying to accomplish. For example:

- Provide high speed Internet access
- Provide high speed access to internal network / systems
- Deploy a high performance video surveillance solution
- All of the above?

Does the customer have a specific use case?

- City Wide Coverage
- Campus Networks

- Hotspot Coverage
- Multiuse Networks
- Video Backhaul
- Distribution Centers
- Airports
- Ports
- Public Safety

2.3 Customer Throughput / Coverage Requirements

Once the customer use case is understood the next step is to determine the throughput and coverage requirements of the network.

2.3.1 Throughput

Throughput requirements will depend on the customer's use case. Ultimately, the wireless network supports user data applications, such as telemetry, web browsing, e-mail, video, and file synchronization. Application requirements enable the specification of throughput as part of the wireless network design. Initial understanding of the specific use cases and the applications that will be supported on the network will help determine what the actual throughput requirements are. When determining throughput requirements consider the following:

- For Internet / Internal network access
    - What radio frequency will be used for access?
    - Are all of the clients 802.11n? Is there a mix of legacy clients?
    - What is the expected throughput per client?
    - What is the predicted simultaneous number of users per AP?
- For video applications
    - Number of simultaneous video streams per AP?
    - Throughput required per video steam?
    - Will the streams be multicast?
    - What video Codecs will be used?

- For custom applications
    - Throughput required per application?
    - Average packet size used by application
    - Are there specific latency requirements?
    - Is the traffic TCP or UDP?
- Oversubscription Ratio
    - Will there be an oversubscription ratio per AP?
    - Dependent of the number of simultaneous users
    - For example 25 simultaneous users with a 4:1 oversubscription would plan for 100 users per AP.
- Future Growth
    - What are the anticipated growth requirements?

2.3.2 Coverage

Coverage areas define where users will need to access the wireless network. This will also depend on the customer's use case. In most cases the network should be designed to cover only those areas in which coverage is needed. When determining coverage areas consider the following:

- Is 100% wireless coverage required (e.g. city wide)?
- Is coverage required in populated areas only?
- Is only hotspot coverage required?
- Is coverage required along major roadways?
- Is coverage expected inside buildings?

It is important to understand that high throughput / coverage use cases will require more APs. Client devices typically operate at lower power levels and often only have a single antenna. While it may be possible to space APs farther apart, clients may be limited to using lower data rates in areas between widely spaced APs. Thus, when considering a deployment that requires high throughput, APs should be deployed such that the coverage area will allow clients to obtain higher data rates.

2.3.3 Setting Expectations

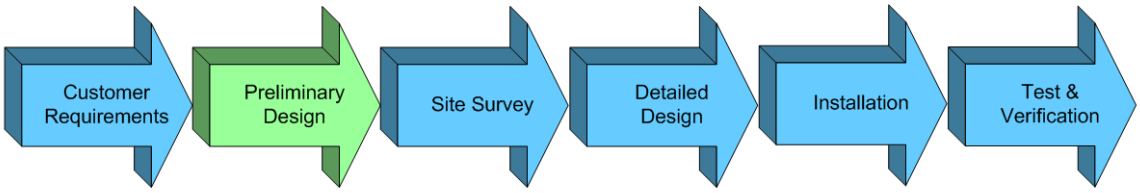
Set the customer's expectations prior to beginning the project. This is very important when creating and defining an Acceptance Test Plan (ATP). You do not want to design and implement a solution only to discover that the customer's expectations are not obtainable or even realistic.

Educate the customer up front on:

- The solution capability e.g. capacity, scalability, etc.
- The expected performance (e.g. throughout, range, etc.)
- The challenges of outdoor deployments
- Networks

Make sure that expectations are documented and understood.

2.4 Preliminary Design



Before getting into the specifics of the preliminary design it is important to understand the realities associated with planning a network. Networking planning is more than choosing points on a map and using selecting node locations at a fixed distance.

2.4.1 A Perfect World

In this first example we see a single AP at the lower corner of a 1 mile x 1 mile grid. In a perfect environment, one can estimate the coverage areas that would provide different levels of performance. The red area would denote a region where the highest MCS rates would be supported thus providing the highest throughput within the coverage area. Father away from the AP the overall SnR for between APs drops thus the available supported rates is also decreases reducing throughput.

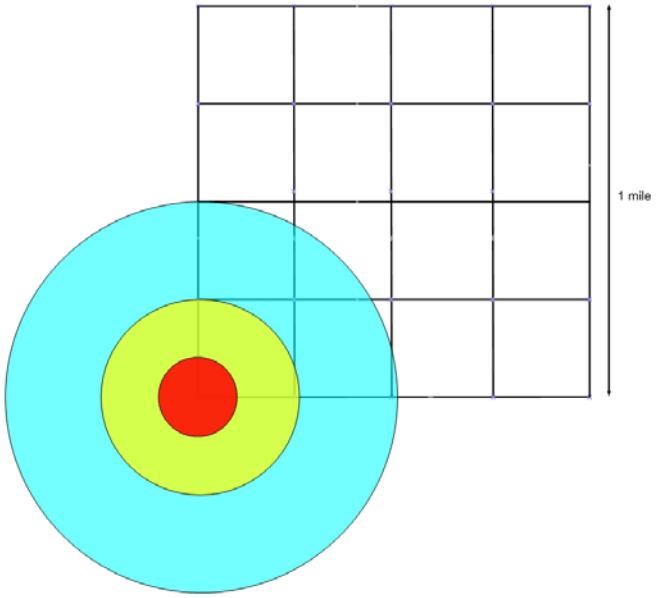


Figure 2-1

The next figure shows a second AP located approximately ½ mile from the first. In this perfect world scenario we see that only the outer coverage band overlaps. In this deployment scenario, while performance could very well still be within acceptable limits, the APs would need to be closer to achieve higher performance (at the expense of coverage).

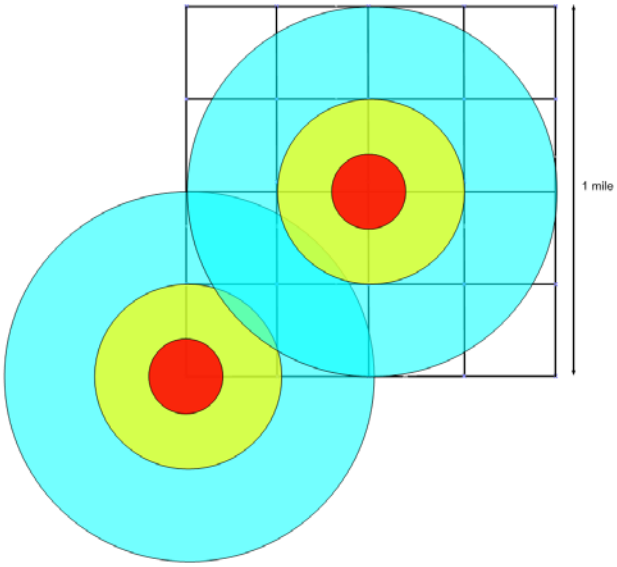


Figure 2-2

In the next figure the second AP has been relocated ¼ mile away from the first AP. Here the second coverage band overlaps thus higher performance will be possible between these APs. (Note that the outer band has been removed from the figure)

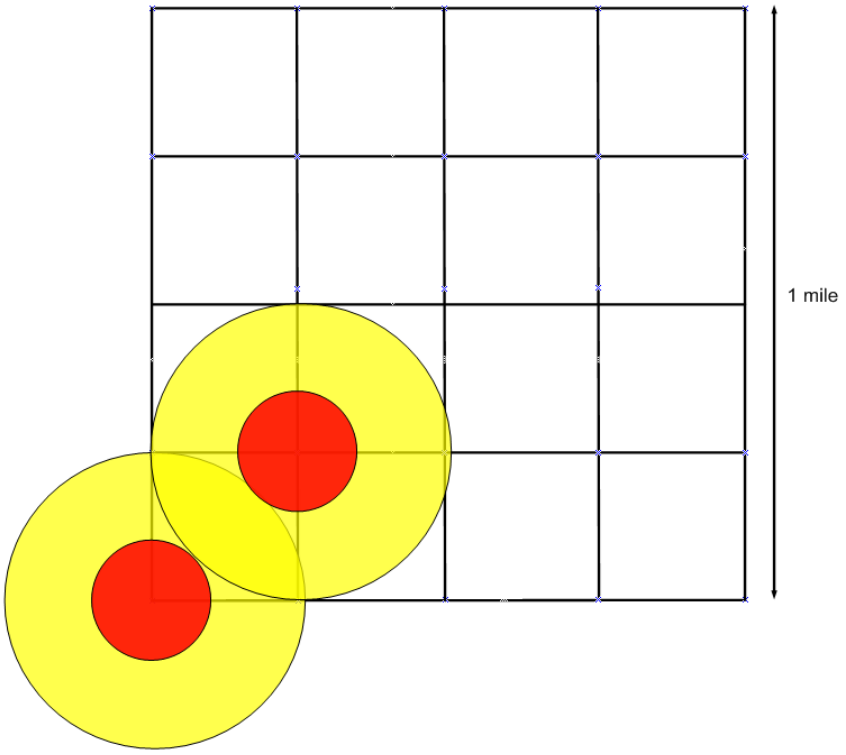


Figure 2-3

In the next example the second AP has been relocated with .1 mile of the first AP. Within this distance the highest MCS rates, thus the highest performance can be obtained (note that the two outer bands have been removed for clarity).

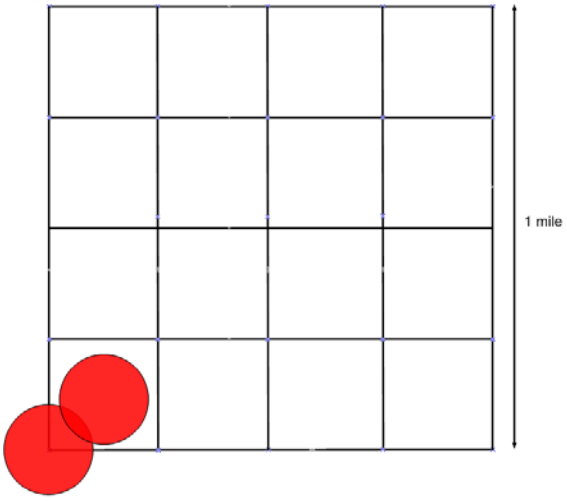


Figure 2-4

2.4.2 Reality

In reality coverage areas can be very different with the previous circle plots. The figure below shows the first AP again however obstacles in the environment have changed the coverage areas.

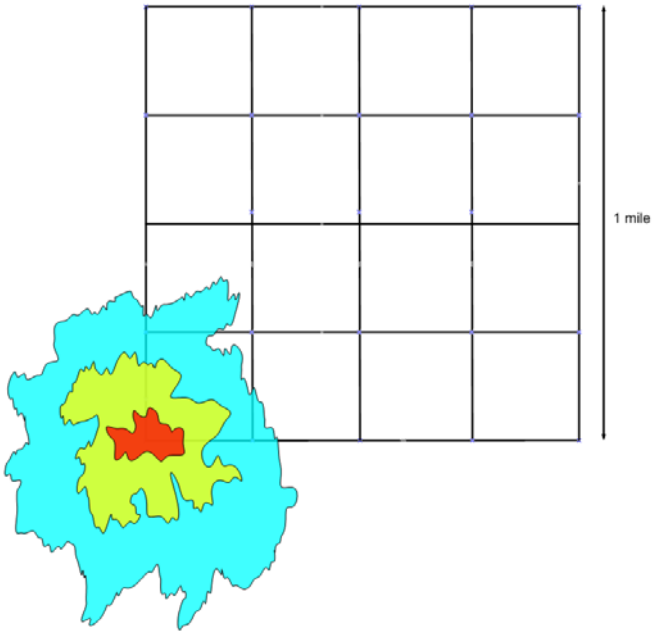


Figure 2-5

In the next figure we see the second AP located ½ mile from the first AP. This AP is also surrounded by obstacles which have reduced the coverage area. Here we see that the outer coverage band (blue) of the second AP does not overlap the first AP. While there will most likely be a signal overlap (not shown in the drawing below), performance may not meet expectations thus the seconds AP should be relocated closer in this example.

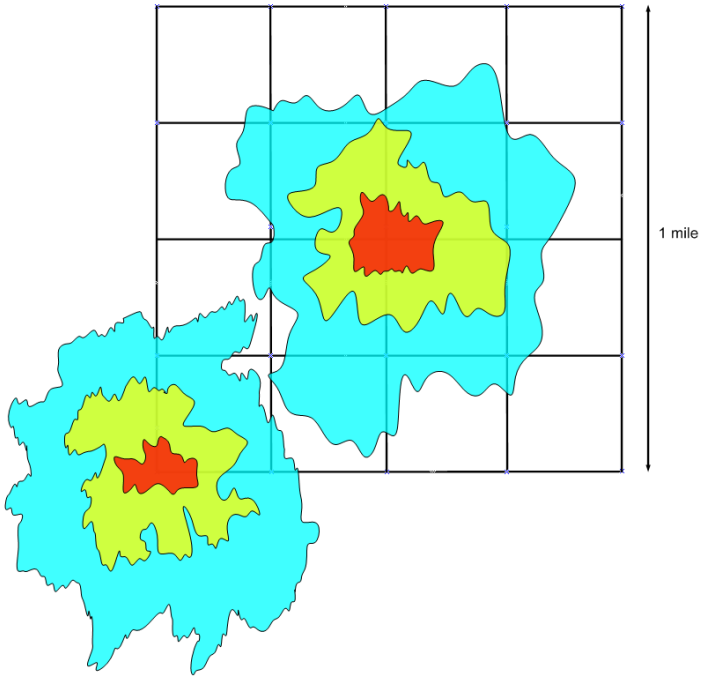


Figure 2-6

In the next figure the second AP has been relocated ¼ mile from the first AP. Here there is some overlap of the second coverage band (yellow) thus higher performance will most likely be obtained.

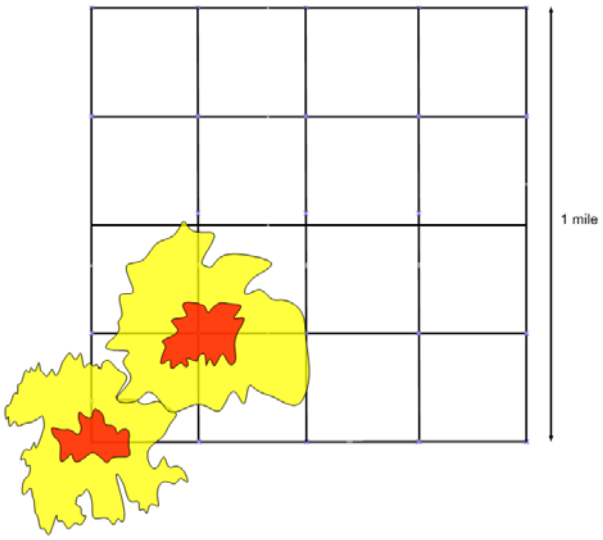


Figure 2-7

Reality is often very different than what was initially planned. In the figure below, an AP has been mounted in a downtown location. Due to the multiple obstructions, e.g. buildings, trees, etc. coverage is very different from a circle plot. In this example, more APs may be required to meet coverage requirements. Also, in an environment like the one shown below multipath can play a significant role in affecting coverage and throughput (multiple spatial streams). Another factor to consider is potential

interferers located within buildings along the coverage route. A good site survey can provide a snapshot of potential sources.

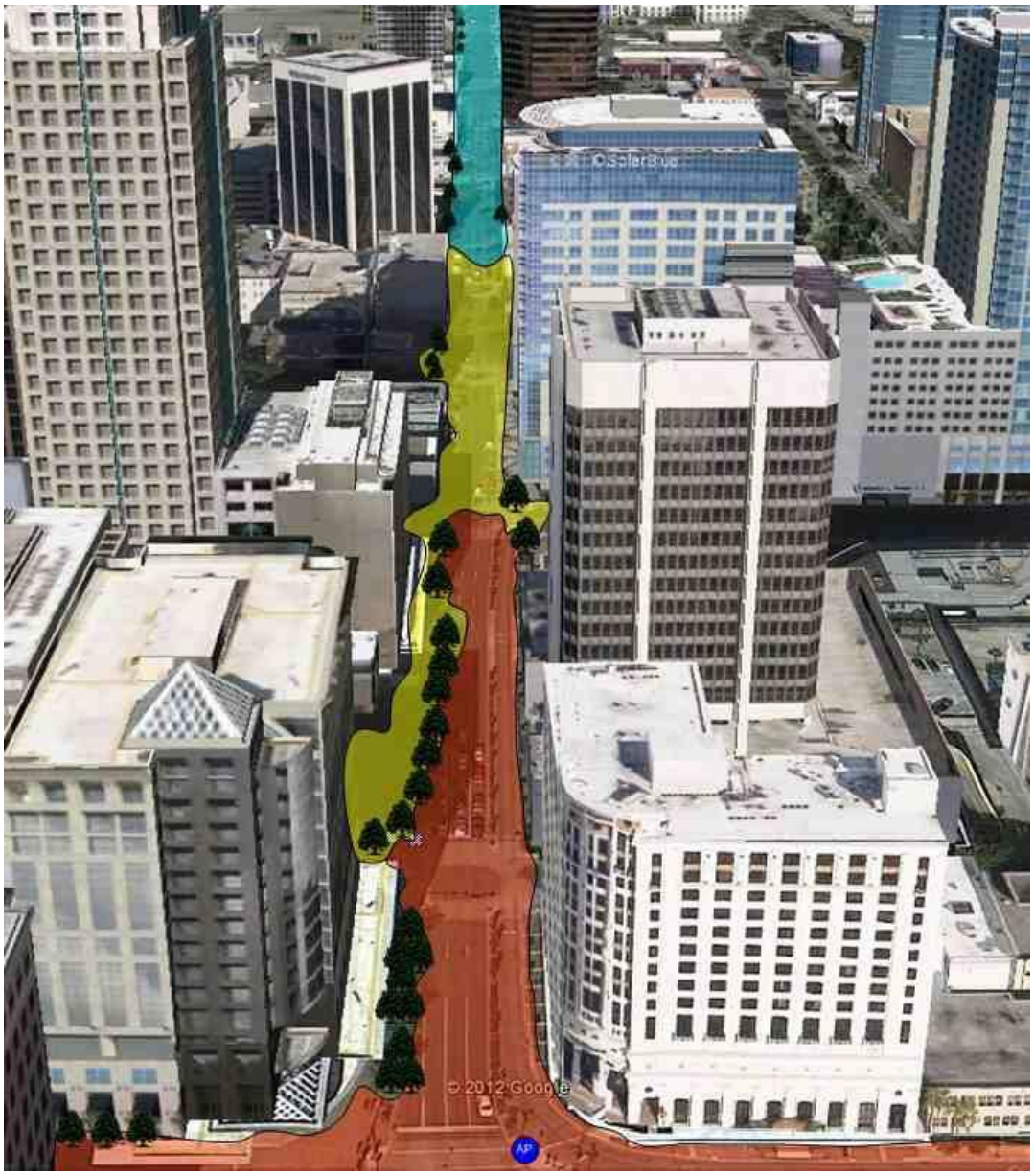


Figure 2-8

2.4.3 Identify Coverage Area

As discussed in section 2.1.2 the coverage area needs to be identified. For example in the figure below coverage is required in the downtown area, the local park, and the warehouse district. Coverage is not required between these areas. The network designer would focus on the throughput and coverage requirements in these specify areas only.

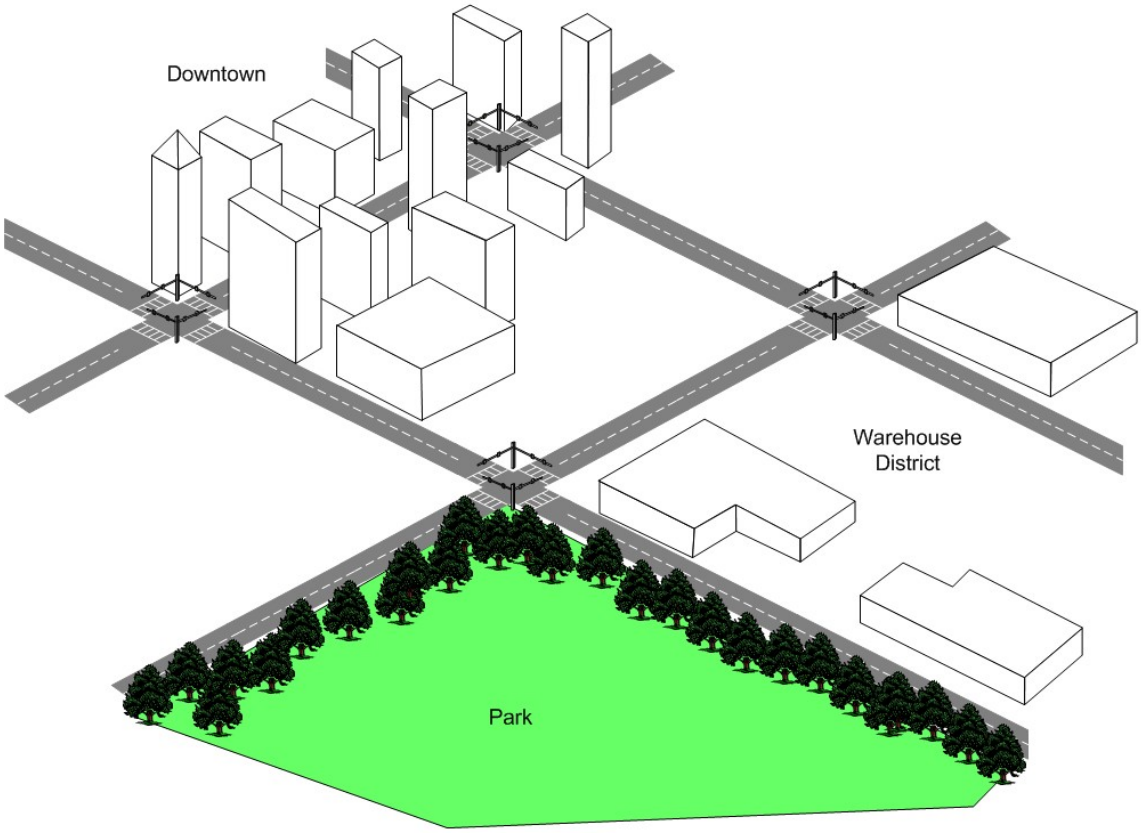


Figure 2-9

2.4.4 Estimate Number of Devices Required

2.4.4.1 Root Devices

Within a coverage area estimate the number of Root (wired APs) will be required. To determine this network operator must estimate the number of peak users and the throughput requirements of each user. The backhaul connection available to the Root device must also be taken into account as this connection will be ultimately shared by all clients connected to the Root and clients connected to each Mesh AP under the Root.

Root backhaul connection = 50 Mbps
User requirement = 500Kbps
Backhaul can support 50,000,000/500,000 = 100 simultaneous users

Thus if 200 peak users each requiring 500Kbps then at least 2 Root devices will need to be deployed within the coverage area. While these users may be spread out across multiple devices (including Non Root APs) ultimately 2 Root devices in this example will be required to support throughput requirements.

2.4.4.2 Non Root Devices

In the previous section it is shown how throughput is injected into the network by adding Root devices. Wireless clients can connect to Root devices thus coverage is also added by each Root device. Non Root devices (non wired APs) meshing to Root devices inject coverage zones into the network. In the distribution center example below we see a single Root device, a 1 hop Non Root device and a 2 hop Non Root device. The Non Root devices were required to extend coverage around the distribution center.

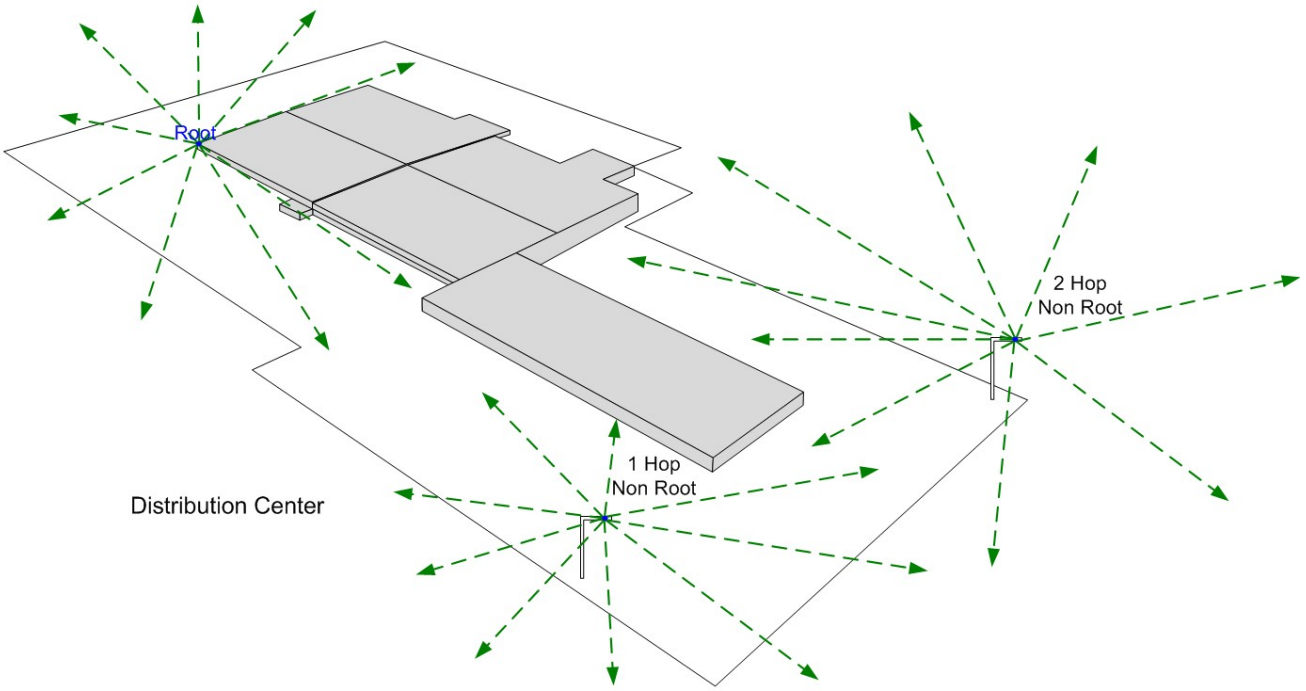


Figure 2-10

Note that each AP7161 can support up to 256 wireless clients (256 - # mesh neighbors). When planning the capacity of a coverage area an over subscription factor is sometimes applied. For a single AP7161 with a 2:1 oversubscription factor would provide panned coverage for 512 wireless clients.

2.4.5 Identify Available Mounting Assets

When planning the preliminary design take notes of the available mounting assets available in the required coverage areas. Look for available assets such as:

- Traffic poles
- Telephone poles
- Power poles
- Buildings

Ideal assets will allow all devices to be mounted at 30-35ft and have clear line of sight between devices.

When planning your coverage area note that intersections along roadways are often good choices for mounting locations. Intersections generally offer coverage corridors in multiple directions.

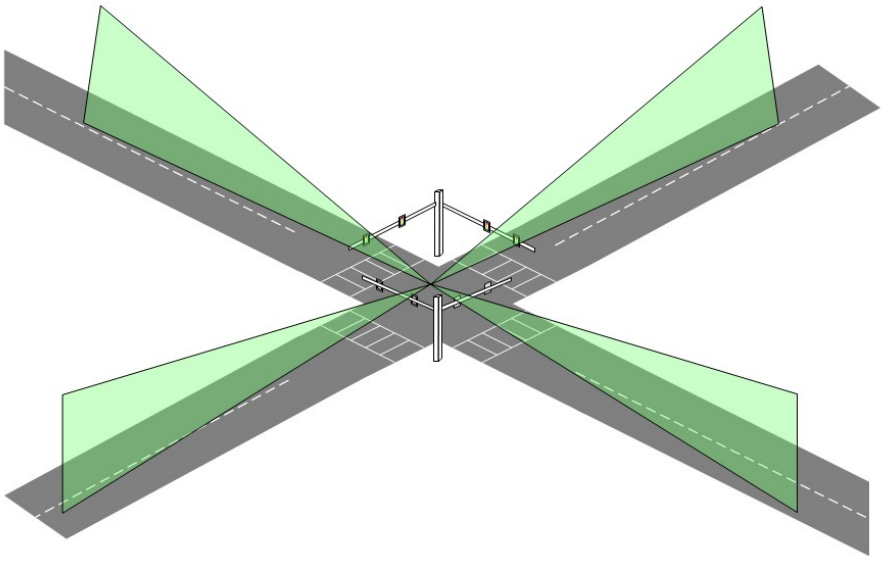


Figure 2-11

When planning coverage using assets along roadways devices should be placed on alternate sides. This generally provides better line of site visibility between devices.

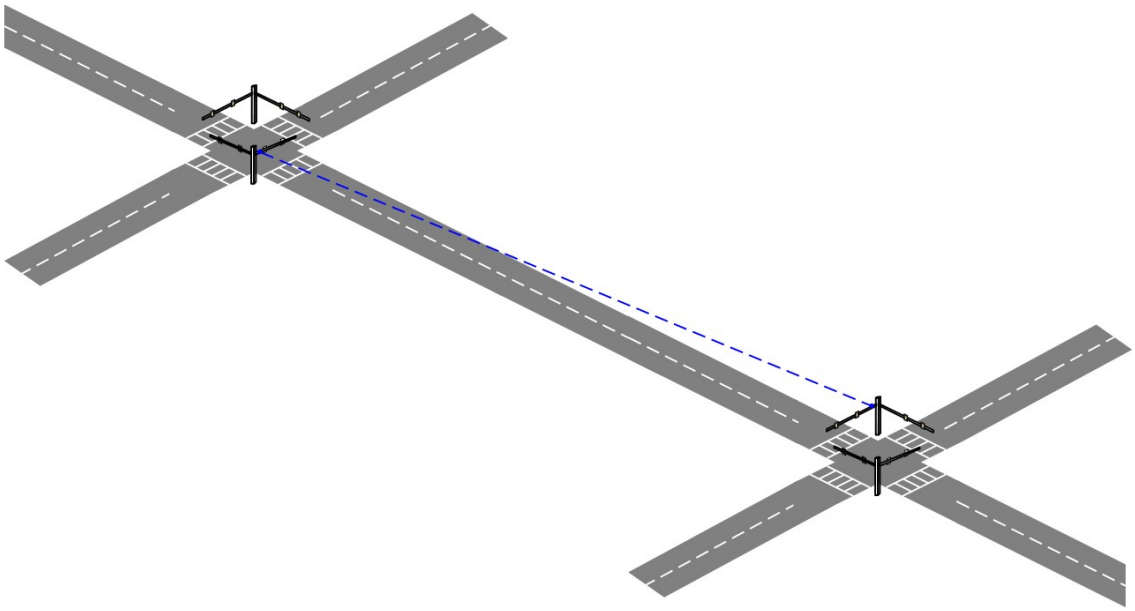
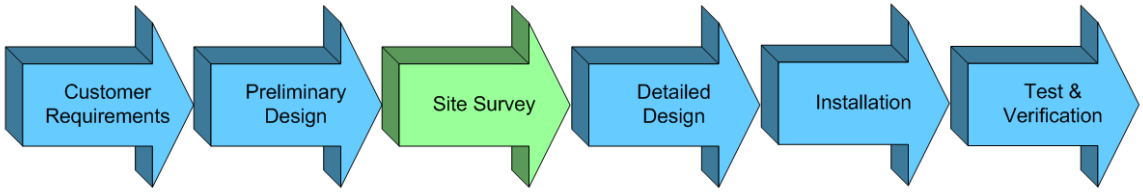


Figure 2-12

2.5 Site Survey



The following information should be obtained from site survey:

- Land drawings and building database plus geographical coordinates/referencing (if available).
- Wireless connectivity points (point of entry for Ethernet).
- Power connectivity points
- Equipment rooms
- Outline of the areas of coverage
- Potential AP7161 locations
- Interference levels at the test point locations

An initial site assessment involves a preliminary assessment of the coverage area. The following information can be obtained using information provided by the customer agency:

Obtain a map of the desired coverage area

Contiguous coverage is typically required over the desired deployment area. It is important to identify regions where contiguous coverage is required, and where coverage is not required.

Contiguous coverage means a deployment region where no coverage gaps exist over the intended coverage area. For the wireless mesh networking solution, where the intended use is for wide geographic area coverage such as metropolitan area coverage, this may typically mean dozens of Client APs around a coverage region.

Identify existing power sources and network equipment

This includes identifying the location of wiring closets, LAN switches, and uninterruptible power supplies. Are there existing 802.11 APs that must coexist with the wireless mesh network? Are existing wireless services deployed at the site (e.g., known sources of interference, like Bluetooth PANs)?

Obtain network diagrams for existing customer networks

This includes IP networking diagrams to understand the context of the existing network. Although this information relates primarily to integrating networking services with the new wireless network, this

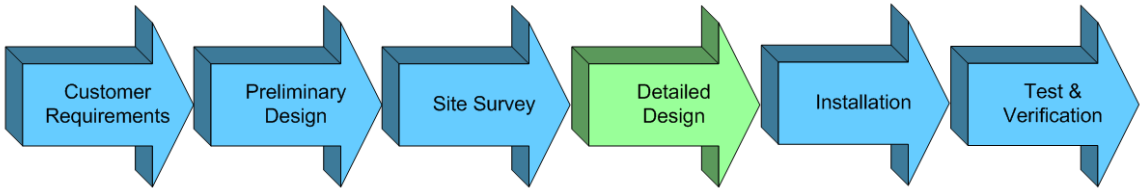
information aids in determining the potential physical wireline connectivity of the APs, as well as network naming conventions employed.

Topology diagrams can also help to identify any need for wireless bridging. A site survey involves a visit to the customer site to identify characteristics of the coverage area, including availability of electrical distribution or existing network infrastructure. The site survey will involve preliminary WLAN measurements to identify candidate AP locations. When scheduling a visit to conduct a site survey, request access to wiring closets, adjacent floors, and other locations that may require special permission.

The following information should be obtained by physical inspection of the site (the goal is to verify and complete the facility map):

- Collect details on wiring closets, power sources, elevators, and support columns.
- Seek out potential barriers to radio propagation, such as metal blinds, fire doors, solid core walls, and radiographic equipment.
- While a hardware based spectrum analyzer provides the best frequency footprint free tools such as inSSIDer™ and NetStumbler™, (and many others) provide a basic view of frequency use.
- Take measurements at ground level as well as at the height devices will be mounted
- Determine whether any radar interferers exist in the environment

2.6 Detailed Design



2.6.1 Effects of Terrain / Foliage

Coverage is defined by the geographic region for which a subscriber device is able to receive an acceptable minimum service level (e.g., can send data successfully at the lowest available data rate). Coverage is synonymous with an ability for an end-user to achieve a minimum data throughput rate at a particular geographic locale (e.g., at a certain distance - or range - from the AP7161). Such quantitative assessments are often complex, since at the 2.4 GHz frequency of operation, RF propagation effects that contribute to the achievable signal-to-noise ratio can vary dramatically in outdoor environments.

The following factors impact signal-to-noise ratio:

- Free-space propagation loss.
- Distance and frequency.

- Penetration loss.
- Receiver sensitivity.
- Interference.
- Client device transmit power.
- Destructive Multi-path interference (Note that with 802.11n multipath can enhance performance via spatial multiplexing).
- Shadowing.
- Fading (Doppler/Rayleigh).
- Antenna configuration.

In general, Zebra recommends that wireless mesh infrastructure devices are deployed predominantly line-of-sight (LOS) to maximize the wireless network capacity. In this way, the non-deterministic fading channel impairments, of aforementioned factors that impact signal to noise, are minimized.

Coverage goals should be to cover where the population is, not the unpopulated areas. Most coverage areas are comprised of zones with different density. Terrain will greatly impact the coverage of a mesh network.

2.6.1.1 Rural Flat / Minimum Foliage

In rural environments it is easier to obtain line of site. Devices can usually be placed father apart. The RF environment is generally less complex and more predictable.

2.6.1.2 Suburban / Mild Building Foliage

Suburban terrain tends to be a mixture of open spaces and dense obstructions. The number of devices required for coverage may vary greatly depending on location specifics. There may be areas in which more nodes may be required due to dense obstructions.

2.6.1.3 Urban / Heavy Building / Foliage

In a dense urban environment with a lot of obstructions node density will usually be much higher. Dense areas tend to create more complex RF environments. Performing site surveys will be required to ensure optimum device placement.

2.6.2 Selecting Root AP Locations

AP7161 APs attached to the wired network are considered Root devices. Root APs serve as gateways between the wireless mesh network and the wired network. **Root AP locations should be determined first** since they control the critical function of routing to and from the wired network. Root APs must have an Ethernet connection to the core network. The AP7161 Ethernet ports support 10/100/1000 Mbps

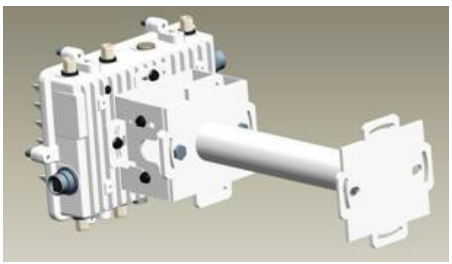
Ethernet connections. If direct Ethernet is not available or within distance requirements of the core network wireless backhaul technology such as Point to Multi Point or Point to Point systems can be used. When using a wireless backhaul careful planning must be performed to ensure that the wireless backhaul does not interfere with the AP. When operating on the same or adjacent frequency band adequate horizontal and vertical separation must be observed when locating the wireless backhaul near the AP. Typically 20 or more feet is sufficient.

Common mounting locations for the AP7161:

- Light Poles / Utility Poles / Traffic Poles
  - Will require power company / county agreements
  - Power usage (32W average, 36W peak / dual radio 70% duty cycle)
  - Wind loading (AP7161 rated at 150 mph)
  - Is grounding available?
  - 24x7 power available?
- Buildings / Towers
  - May require lease agreement

It should be noted that it is incumbent upon the customer to obtain the required Pole Attachment Agreements for devices to be installed on traffic / utility poles. Obtaining the agreements can be a lengthy process, so ample time must be allowed for this process. The potential pole locations should be logged with GPS obtained coordinates along with any identifying numbers on the pole, so that this information can be conveyed to the appropriate utility agency. It is also recommended that alternate mounting locations be located as the utility agency may not allow the mounting of a device at a desired location. Also, it is not uncommon that multiple utility agencies operate within the same community and this coordination must be taken into consideration. In addition, it should be verified that light pole selections have power available 24 x 7 and the power available is within the operational range of the device being connected. Specialized brackets may be required for attaching devices to decorative light poles and these brackets may have to be custom fabricated. If this is the case, allow enough lead time for the fabrication of the required brackets.

Device locations should be chosen such that antenna are at least 30 inches from any nearby metal poles to avoid distortion of the RF pattern (**use the available extension bracket (KT-150173-01 if required**). The antennas must



also have a separation distance of at least 2 meters from the body of all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Use wireless backhaul from any location without accessible wireline connectivity to the Root AP. In most cases the Root AP and the wireless backhaul device can both be mounted on a utility pole.

AP7161 devices are IP67 rated. An IP67 enclosure is rated against falling dirt, rain, sleet, snow, wind-blown dust, water immersion (under defined conditions), and corrosion; and will be undamaged by the external formation of ice on the device.

Typically, roadways in the deployment area become main arteries for the wireless mesh network. Roadways can provide line-of-sight coverage over large distances between Root and Client APs. A wireless site survey should be done to identify optimum AP placement.

Steps in Root AP Planning

- Identify Root AP locations / mounting assets in the required coverage area
    - □ Verify the asset can support the weight and wind loading requirements of the AP / mounting bracket.
    - □ Verify power is available at Root AP location.
    - □ Verify line of site from mounting location to potential Non Root AP mounting locations.
    - □ The recommended mounting height 30-35ft.
    - □ Verify that the Root AP can be mounted such that the antennas will not be near any metal objects
    - □ Factor in site survey data when selecting potential locations. You would not want to mount an AP in the path of a strong interferer such as a Point to Point radio link
    - □ Obtain permits and or lease agreements.
    - □ Verify site location availability e.g. can the mounting location be visited after hours?
- Identify Root AP backhaul technology (Ethernet, PTP, PMP, Fiber)
    - □ Root APs with a wireless backhaul usually backhaul traffic to a cluster point e.g. PMP
    - □ Wireless backhaul clusters can be on towers, rooftops, etc.
    - □ Ensure Root APs have line of site to these cluster points

2.6.2.1 Selecting a Backhaul Technology

In most deployments, Root AP7161 cannot be directly connected to the core network. Thus a wireless backhaul link is needed to connect to the core network.

Depending on the use case and deployment environment, there are multiple backhaul technologies available to use with the AP7161. This includes wireline based and wireless based.

Criteria to choose a backhaul technology include:

Throughput requirements

The designer needs to consider what the UDP/TCP throughput the AP7161 will be delivering to the core network.

For example, you may design the network for video surveillance to carry multiple high quality video streams which require a total UDP throughput of more than 50 Mbps. In that case, you should consider using high capacity fiber link or high capacity PTP link.

On the other hand, you may take advantage of the longer range of 802.11n technology to design a low cost, high coverage solution for the customer. In that case, total throughput requirement for the AP7161 to the core network may be in the range of 10 to 20 Mbps. A PMP based link may just be an ideal solution to fulfill the need to bridge the AP7161 Root with the core network.

Availability of wireline backhaul

Fiber and straight Ethernet connection would always be a good choice to consider if they are readily available at a reasonable cost. These kinds of connections would typically provide high backhaul capacity for the Root APs.

Another choice would be existing telephone lines. By using the private broadband network (PBN) products, the AP can be connected to the core network with medium throughput capacity.

Availability of wireless RF resource for backhaul

When choosing wireless link such as PMP based or PTP based, the system designer needs to consider the available RF band for use in the overall system, making sure that the RF band is not being used by other system that will cause interference to the deployment.

Deployment environment suitable for wireless backhaul

When determining whether a wireless backhaul technology can be used, the system designer needs to take into account on whether line-of-sight (LOS) is achievable for the backhaul link. If LOS is not achievable, will near-line-of-sight (nLOS) or none-light-of-sight (NLOS) provide enough link budget to deliver the desired backhaul throughput?

2.6.2.2 Wireless Based Backhaul Choice

Zebra partners such as Cambium Networks provide a broad range of wireless backhaul technologies that can be used for the AP7161 deployment. When choosing a wireless backhaul technology, the system designer needs to consider the deployment use case.

For example, if the mesh system is designed for high cluster throughput using a 40MHz channel size, the cluster may provide an overall capacity of up to 300 Mbps raw data rate. In that case, a Cambium Networks' PTP 600 backhaul link may be required to match the mesh layer throughput requirement.

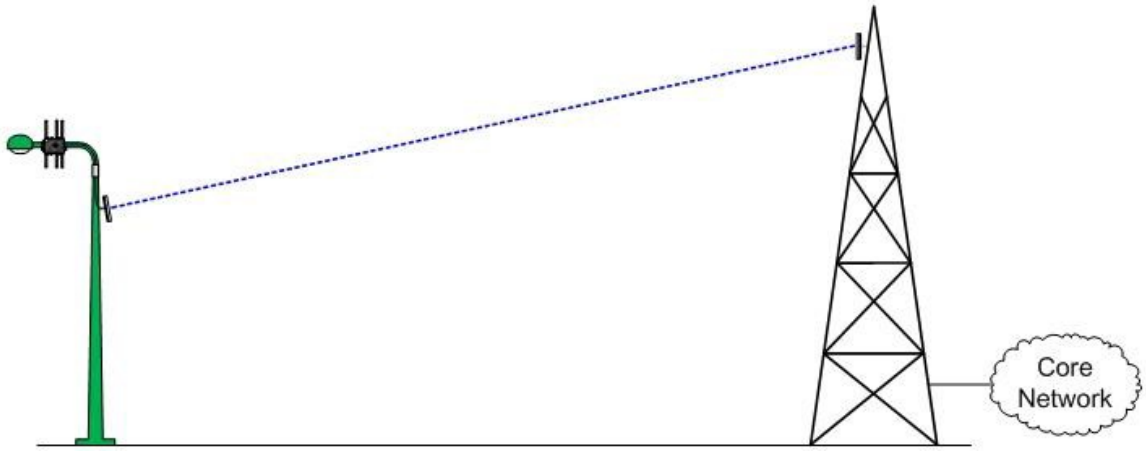


Figure 2-13

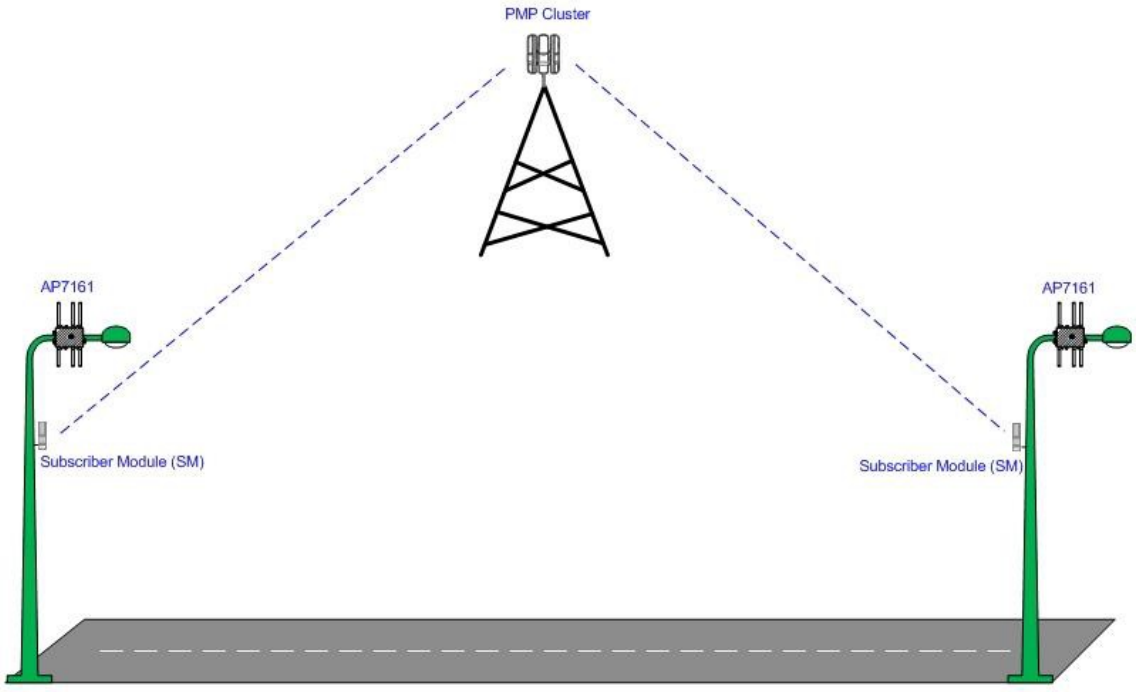


Figure 2-14

If the mesh system is designed for low cost, high coverage scenario that longer range is used to trade for high throughput, depending on the overall capacity requirement for a cluster, one may choose to use

Cambium Networks' PTP 200 technology as backhaul which provide a backhaul throughput of only up to 50 Mbps.

The following diagram shows an AP7161 Root AP using a PMP link as backhaul. Multiple backhaul links are concentrated to a PMP cluster where traffic is further backhauled to the core network using a PTP backhaul link.

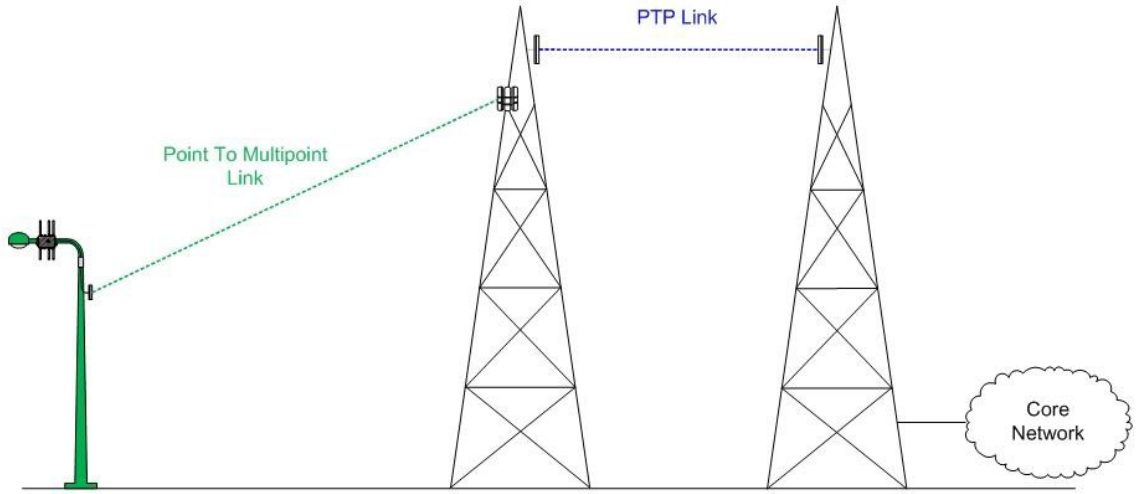


Figure 2-15

2.6.2.3 Collocating the AP7161 and a Wireless Backhaul Radio

When locating a backhaul wireless radio on the same mounting location as an AP7161 Root node adequate horizontal and vertical separation is required to reduce interference. 5 to 10 feet of vertical and horizontal separation is recommended. Also, provide as much frequency separation as possible between the AP7161 and the wireless backhaul radio.

2.6.2.4 Wireline Based Backhaul Choice

Wireline based backhaul choices includes fiber optical backhaul and Zebra Private Broadband Network (PBN) based backhaul.

Fiber optical backhaul is relatively expensive, and requires point of present at the deployment side as trenching new fiber link to the site is costly and it takes longer for the deployment. However, Fiber optical backhaul provides capacity at more than 10 Gbps and has nearly no range limitations. The following diagram shows an AP7161 Root AP using fiber link as backhaul.

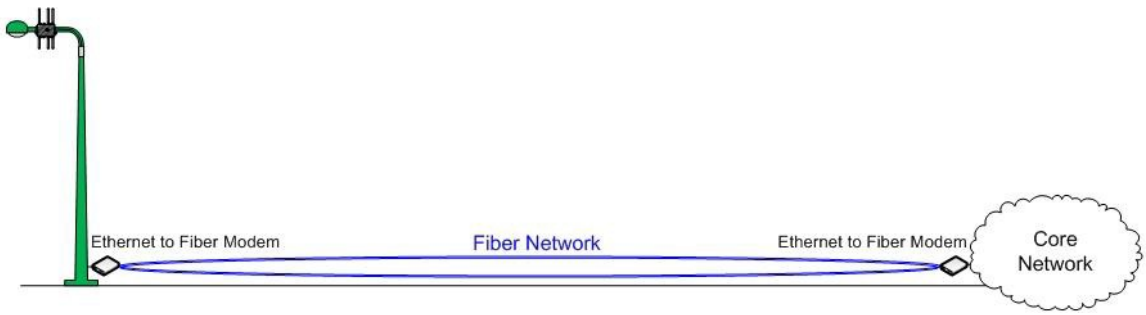


Figure 2-16

Another wireline based option would be the Zebra Private Broadband Network (PBN) solution running on top of existing telephone copper lines. The Zebra XLP 700 Ethernet Extended provides throughput of up to 78Mbps (full duplex), with decreasing throughput over distance. This could be a low cost solution if very high backhaul throughput is not required and if there is telephone line at the AP location.

Figure 2-17

2.6.3 Selecting Non Root AP Locations

AP7161 APs that are not Roots are considered Non Root devices (often referred to as Mesh Points). The placement of Non Root APs will depend on the mounting assets in the required coverage area and follow the same guidelines discussed in the previous section.

- The same guidelines discussed for Root APs apply
- Placement of Non AP locations will depend on available assets around Root APs
    - Non Root APs should be mounted at the same height of 30-35ft.
    - Consider the number of potential hops when planning Non Root AP placement. 3 hops or less is recommended.
- Plan the network outward from each Root AP

2.6.3.1 Fresnel Zone

Fresnel Zone is the football shaped ellipsoid area between antennas. In order to achieve clear line of sight, there should be no blockage in the Fresnel Zone. So it is important to keep this area clear of obstacles to reduce fading in the signal path. The first Fresnel Zone can be easily calculated using the formula showed in the following diagram.

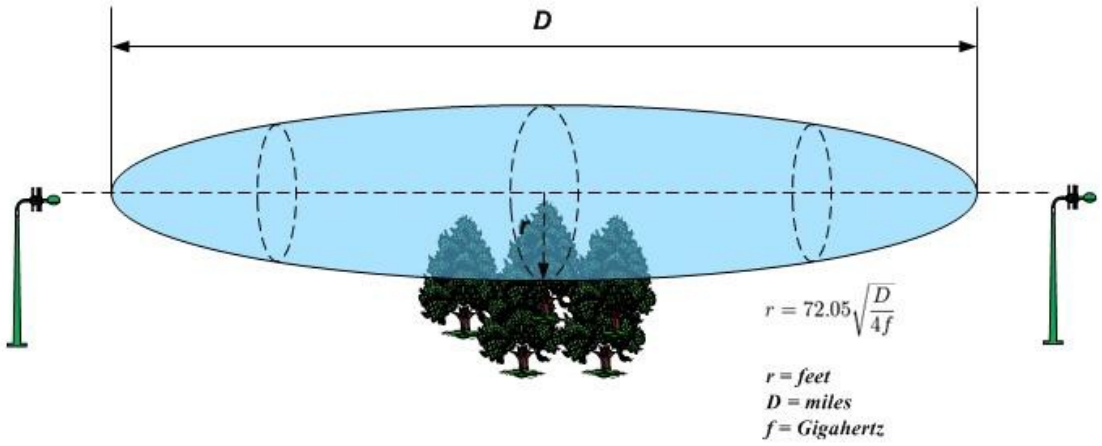


Figure 2-18

As a rule of thumb the area containing the first 60% of the first Fresnel Zone should be clear.

2.6.3.2 Fresnel Example

Two AP7161 are mounted on poles at a height of 30ft.

The distance between these AP7161 is .1 miles

Operating frequency is 2.41 GHz

Calculate the first Fresnel Zone:

r = 72.05 x √ (.1 / (4x2.41)) = 7.34 ft (middle of link)

Radius r height above the ground = 30 - 7.34 = 22.66 ft

Radius r height @ 60 % obstruction:

r = 72.05 x √ ((.6 x .1)/(4x2.41)) = 5.68 ft

Maximum obstruction height in the middle of the link:

Obstruction (max height) = 30 - 5.8 = 24.32 ft

2.6.4 Node Spacing

Typical AP spacing for the AP7161 is .1 to .25 miles. .1 mile is necessary to achieve the highest possible data rates. As with coverage, AP spacing is highly dependent on terrain. For example, dense urban environments with a lot of obstructions will often require APs to be closer together.

When deploying APs in a city, intersections are optimal device locations as they usually offer clear line of site in multiple directions.

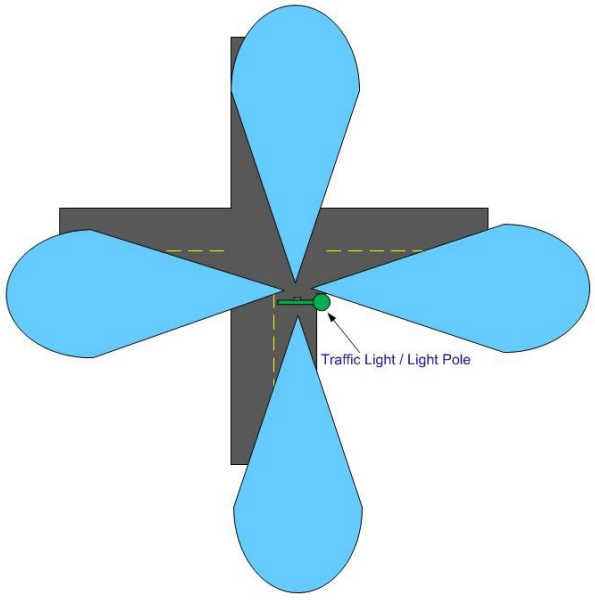


Figure 2-19

When deploying APs along roadways make sure they are placed on alternate sides of the roadway to obtain line of site.

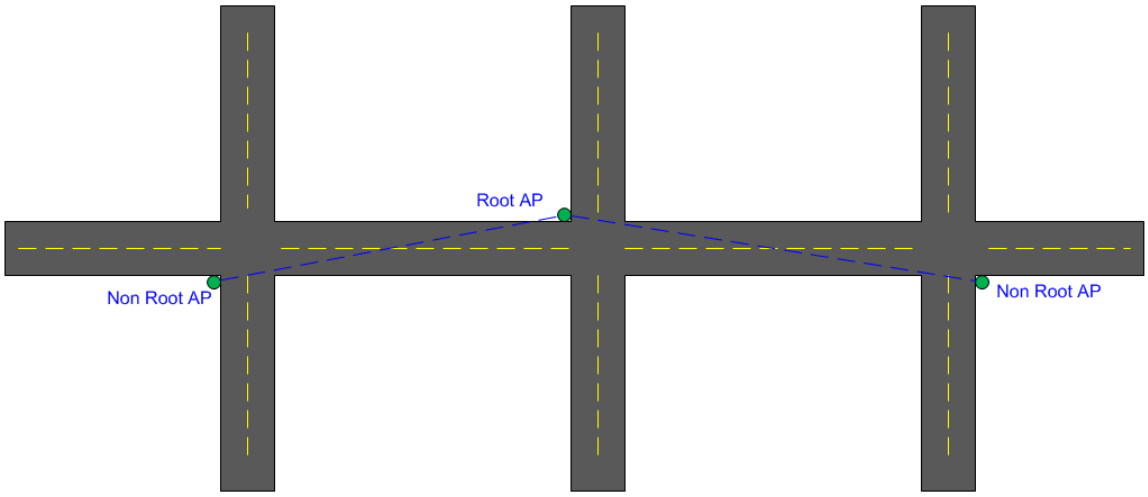


Figure 2-20

2.6.5 AP Height

AP7161 APs are typically mounted at a height of 30-35 ft. Ensure that neighboring APs are mounted at or near the same device height. Excessive height should be avoided as devices will tend to "hear" more 802.11 traffic thus increasing the collision domain.

Guidelines:

- Typical height is 30 - 35 ft
- Avoid excessive height
  - APs may not mesh as expected (see below)
  - APs will "hear" more potential interferers (in particular the 2.4 GHz band)

- For optimum performance make sure neighboring devices have line of sight to each other
- Locate Root APs with wireless backhauls such that they have line of site to backhaul clusters or PTP locations e.g. towers

In the diagram below, notice that due to its close proximity AP 2 is not within the radiating pattern of AP1.

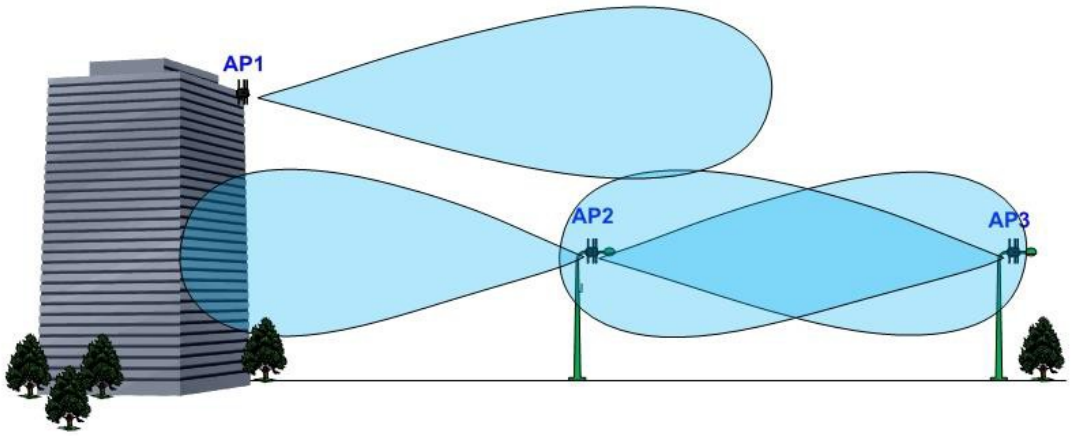


Figure 2-21

2.6.6 Interference

Since the AP7161 operates in the unregulated 2.4 GHz / 5.x GHz ISM (Industrial, Scientific, and Medical) band there is a risk of interference from other 802.11 devices. Other potential interferers include devices such as microwave ovens (more than 100 million in the US alone) and other communications devices such as Bluetooth and cordless telephones. For the 5 GHz band, there are generally fewer sources of external interference. Site surveys can reveal sources of interference and can aid in channel planning.

An 802.11 WLAN analyzer offers the ability to perform spectrum analysis on a per channel basis. When assessing an RF channel, traffic will be seen in bursts on the spectrum, and the energy will only rise as packets are transmitted. With the spectrum analysis capabilities of such a tool, interferers will also appear in the measurement.

- Interference from other 802.11 access points
- Interference from 2.4 GHz / 5.x GHz point to multipoint systems
- Site surveys and channel planning can help mitigate this problem
- Terrain and device height can aid or worsen

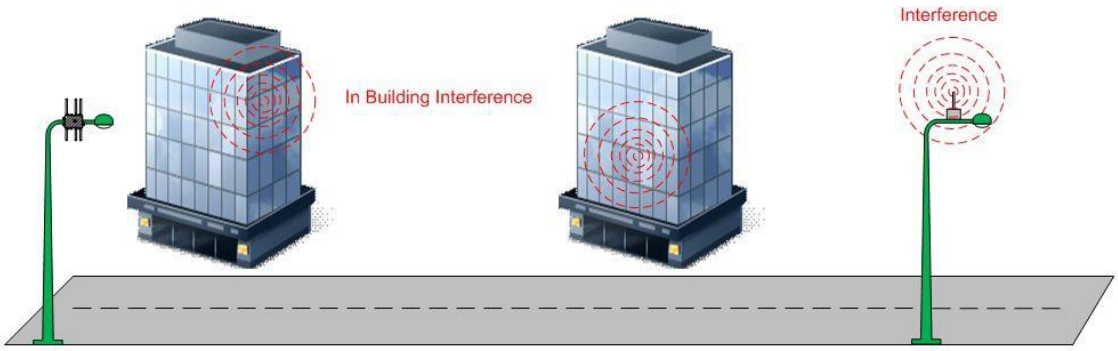


Figure 2-22

2.6.7 Channel Planning

The AP7161 product supports both 20MHz and 40 MHz channel size and works on 2.4GHz ISM band and 5.x GHz band. Understanding what channels are available for use, the deployment engineer would be able to choose appropriate band and channels that best suited the need of the solution.

Channel	Frequency (GHz)	
1	2412	
2	2417	
3	2422	
4	2427	
5	2432	
6	2437	
7	2442	
8	2447	
9	2452	
10	2457	
11	2462	
12	2467	Not Available in US
13	2472	Not Available in US
14	2484	Not Available in US
21	4955	Licensed
25	4975	Licensed

Channel	Frequency (GHz)	
36	5180	UNII Low
40	5200	UNII Low
44	5220	UNII Low
48	5240	UNII Low
52	5260	UNII-2 Mid
56	5280	UNII-2 Mid
60	5300	UNII-2 Mid
64	5320	UNII-2 Mid
100	5500	UNNI-2 Ext
104	5520	UNNI-2 Ext
108	5540	UNNI-2 Ext
112	5560	UNNI-2 Ext
116	5580	UNNI-2 Ext
120	5600	UNNI-2 Ext
124	5620	UNNI-2 Ext
128	5640	UNNI-2 Ext
132	5660	UNNI-2 Ext
136	5680	UNNI-2 Ext
140	5700	UNNI-2 Ext
149	5745	UNII-3 Upper
153	5765	UNII-3 Upper
157	5785	UNII-3 Upper
161	5805	UNII-3 Upper
165	5825	UNII-3 Upper

Please note that the available channels and maximum available power is controlled via a configurable country code. Available channels and maximum power will be automatically configured when the country code is selected. Please see the AP 7161 Product Reference Guide for additional information.

2.6.8 2.4 GHz Band

2.4 GHz ISM only provides three non-overlapping 20 MHz channels. If a 40MHz channel size is planned for 2.4GHz, only one other non-overlapping 20MHz channel is available. The result is a greater likelihood for adjacent-channel interference in the 2.4GHz band. Since channel planning in 2.4GHz was already a difficult task with only three non-overlapping channels in 802.11a/b/g, the use of 40MHz channels is not recommended for 2.4GHz deployments utilizing 802.11n.

The following diagram shows the channels available in 2.4GHz band.

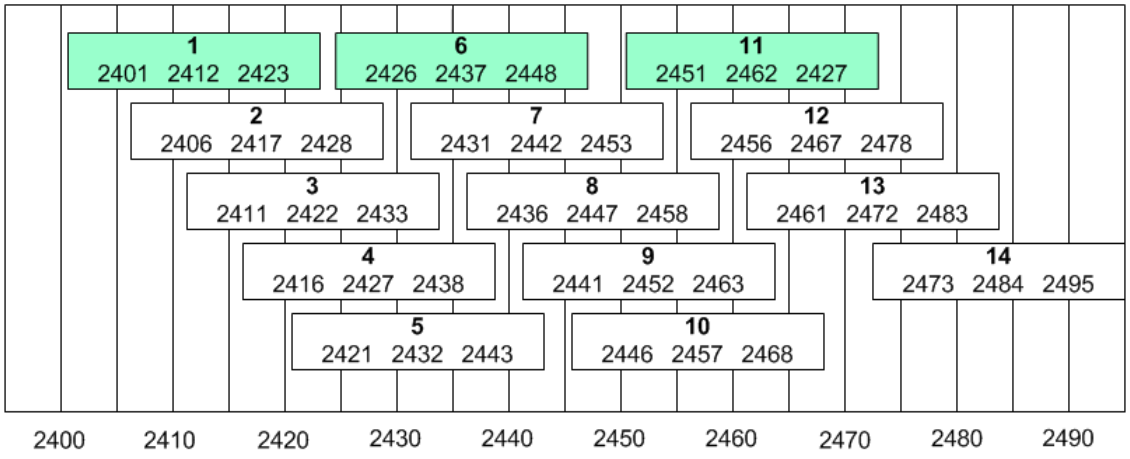


Figure 2-23

If a 40MHz channel is used for 2.4GHz, the secondary channel needs to be adjacent to the primary channel. For example, if Channel 1 is used as primary, the secondary channel should be Channel 6 in order to form a 40MHz channel bonding. If you choose to use Channel 6 as primary, then Channel 1 should be the secondary channel.

2.6.9 5.x GHz Band

The AP 7161 product supports 5.2, 5.4, and 5.8GHz bands. There are nine 40MHz non-overlapping channels across the 5.4 and 5.8 GHz bands.

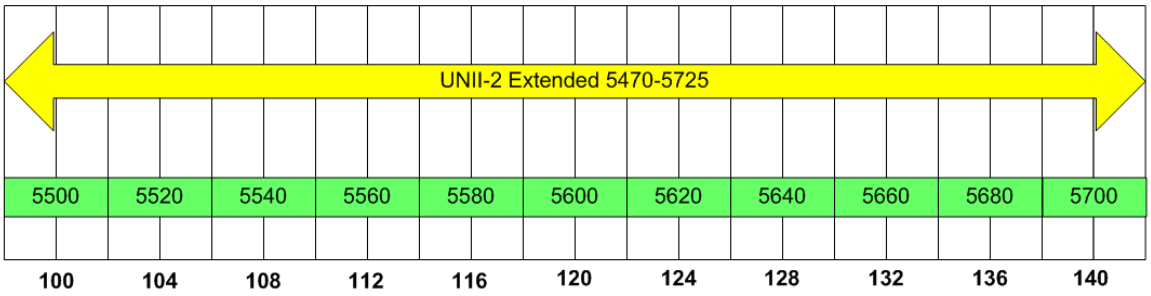


Figure 2-24

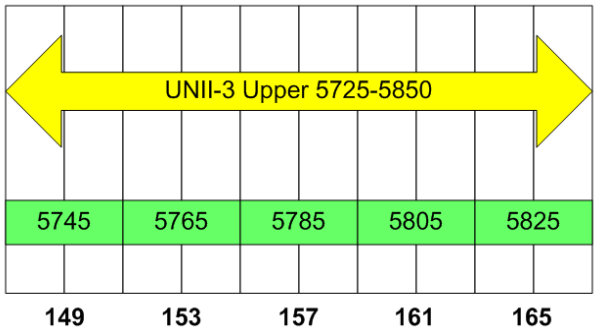


Figure 2-25

NOTE

Transmission power limit could be different for each band. For example, in the U.S, the 5.4GHz (additional U-NII) transmission power limit is only 200mW (29dBm EIRP), while both the 5.8GHz (Upper U-NII) and 2.4GHz (ISM) have a transmission power limit of 1000mW (36dBm EIRP). Also, different countries will have different transmission power and EIRP limitation. Power limits are controlled by a configurable country code.

2.6.10 Auto Channel Selection

The AP7161 can utilize **Smart RF** which enables a user to configure detailed RF channel / power policies. In each radio frequency band a user can configure minimum / maximum power thresholds, which channels to utilize, and the channel width. Smart RF policies can be applied to RF Domains to apply site specific deployment configurations. Please see the **Zebra WiNG 5 Smart RF** how to guide. **Smart RF** also a user to configure detailed scanning options. Non Root APs can be configured with a **Smart RF** policy that ensures they scan for Root APs. The user can also configure a scan interval.

2.6.11 Frequency Planning

Based on an RF site assessment, or by monitoring the channel performance statistics, an RF channel may be selected for system wide use.

The 2.4GHz band is typically used for the access layer and the 5.x GHz is typically used for the mesh backhaul. However, the 2.4GHz band only allows one 40MHz Channel, so it should be avoided if multiple 40MHz channels are needed at the access layer.

When using the 5.X GHz band, one should consider using 5.8GHz (if allowed in the country of operation) if possible since it supports higher transmission power limit (1 Watt) and will have longer range.

A mesh cluster is defined as a cluster of Non Root APs that share the same Root AP. Multiple mesh clusters form a mesh network. In a cluster, all the Non Root APs and their associated Root AP must use the same RF mesh channel. In a mesh network, different clusters may use different RF channels so that mesh clusters can overlay each other to provide higher network capacity. Note that there may be some adjacent channel interference.

Note: A cluster in general is not something this is directly configured. APs with the same mesh radio channel will automatically for a mesh.

2.6.11.1 Access Layer Frequency Planning

There are three ways of planning the frequency at the access layer:

- In this cluster, each AP access layer uses a different channel (color coded in the diagram) from the neighbor AP. **This is the preferred configuration**.

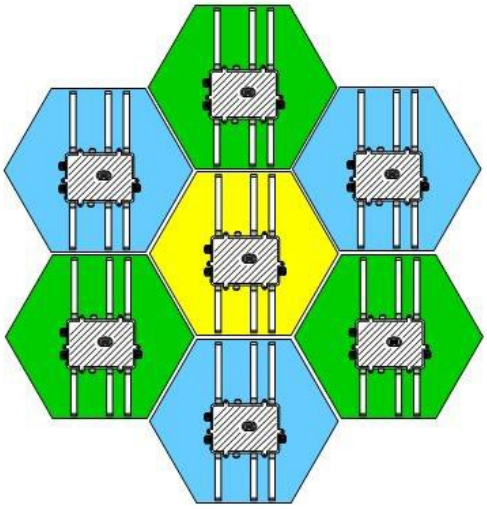


Figure 2-26

- This configuration will provide a higher cluster capacity provided that the mesh backhaul layer does not become the bottle neck. System capacity can be as the high sum of the throughput of all the APs.

- In the next example the same access channel is used within a cluster. The two clusters shown below each utilize a different access channel.

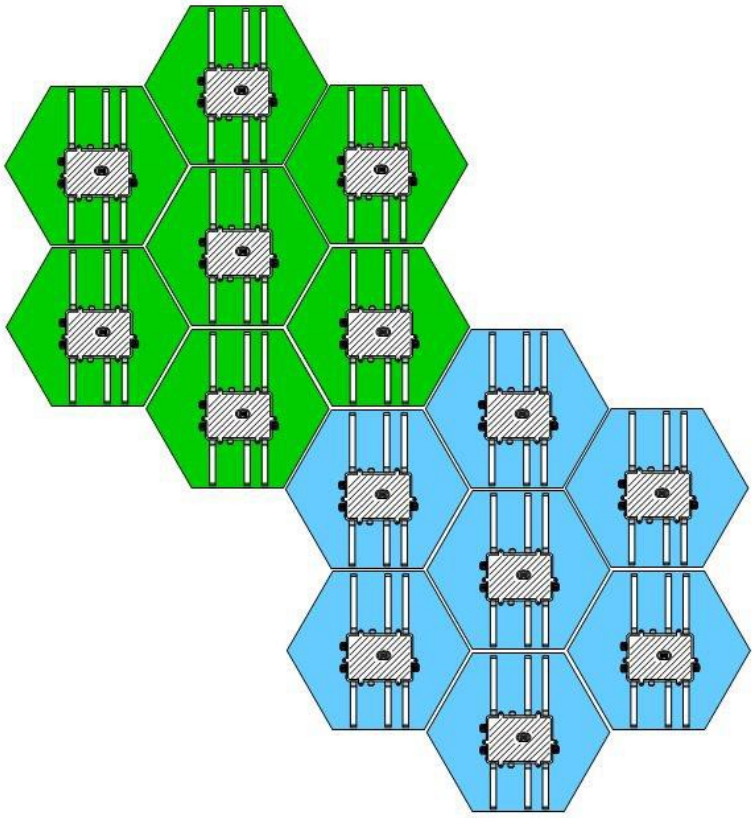


Figure 2-27

In this configuration, the capacity of the cluster will be about the same as the throughput of an AP due to the large single collision domain. This is easier to manually configure, but is not recommended unless there is special use case.

- In this example all clusters utilize the same access layer channel.

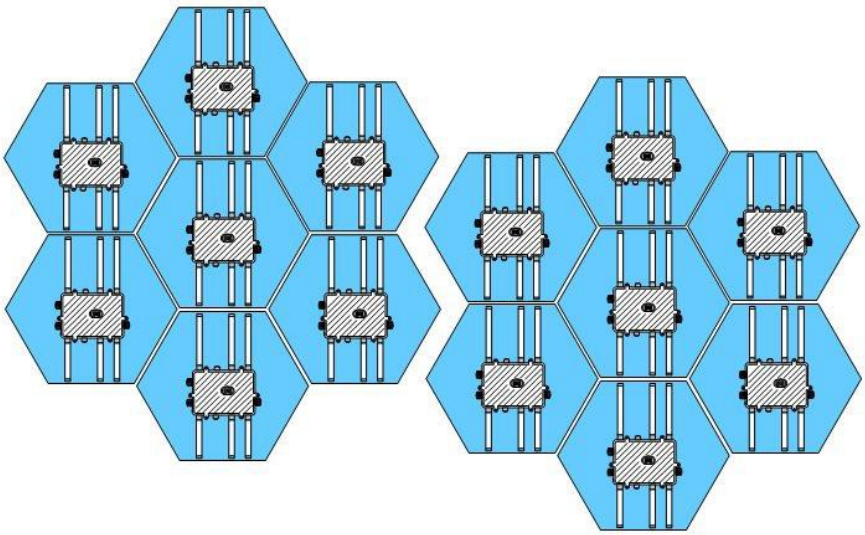


Figure 2-28

This is not recommended unless there is special use case

2.6.11.2 Mesh Layer Frequency Planning

In a Mesh cluster, all the APs have to use the same frequency channel for the mesh layer. But different clusters can use different backhaul channels. Typical deployments would have the network configured so that neighbor clusters use different channels for meshing to reduce interference, as shown in the following diagram:

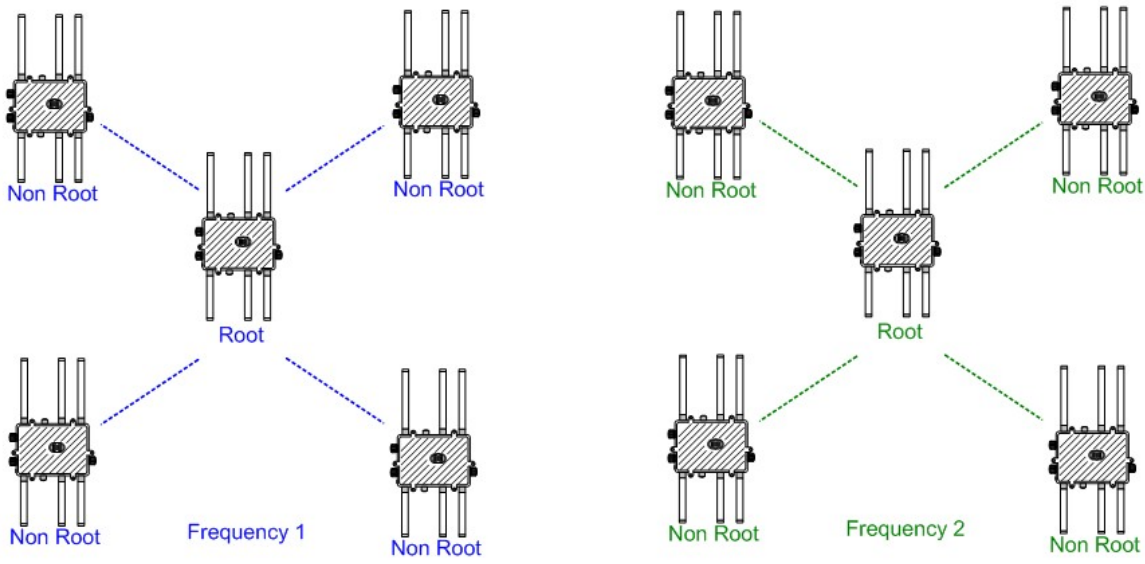


Figure 2-29

To make it easy for deployment, the Mesh configuration interface provides an auto-scan feature, which triggers the Client AP to scan for an unused channel in the selected band. All the Non Root APs will follow the same channel as the Root AP.

The network can also be configured so that all clusters use the same channel for mesh link, as show in the following diagram.

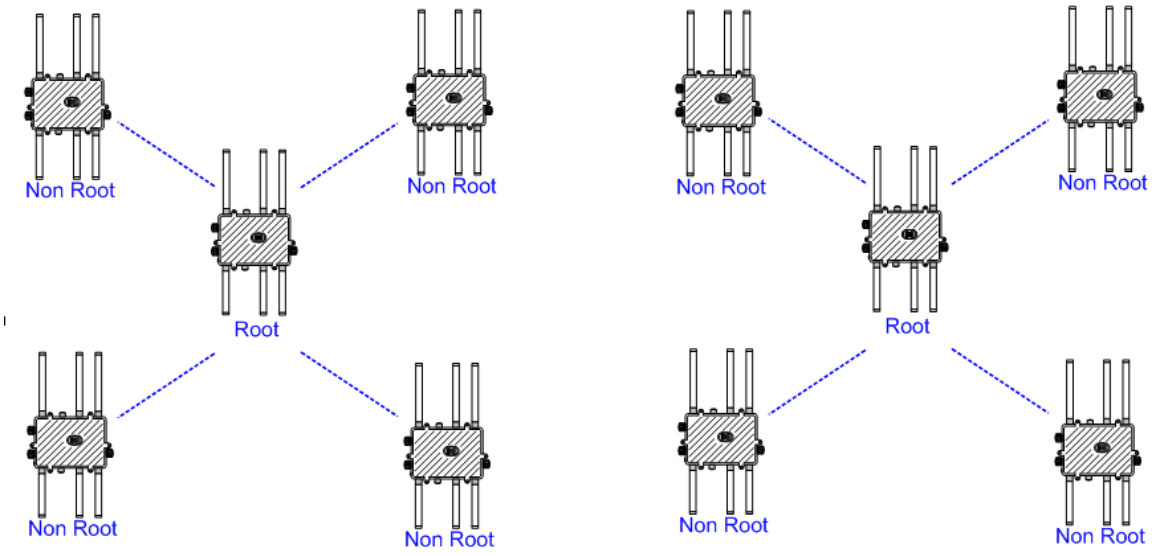


Figure 2-30

This method will limit the overall network capacity since the clusters could interfere with each other at the mesh layer. However, this configuration may be required in mobility solutions. For example, for a vehicle mounted modem configured to mesh on the same channel as the mesh infrastructure backhaul channel. This channel configuration would need to be configured to have a seamless handover in the network (since a VMM configured to auto channel scan would not change channels quickly enough for a seamless handoff).

2.6.12 Capacity Planning

System capacity is the aggregate throughput of a wireless network, which can be mapped to subscriber population capacity (given that the subscriber traffic requirements are known). The wireless mesh network serves end-users through multiple infrastructure points, each simultaneously serving many stations within a given coverage area.

Capacity planning answers the question of "how can multiple mesh devices be deployed to meet the coverage and throughput requirements of a population of users?"

Multiple co-located AP7161 networks could be deployed in a given area provided that the different networks are configured with different mesh credentials. In this scenario channel planning would be critical to minimize RF interference between the co-located networks.

With the operation of multiple co-located networks, the networks appear either as interference to each other or they simply share the same air-interface capacity. This may result in an overall reduced range and capacity of each.

Typically, a system's capacity is the sum of the capacity of each mesh cluster if the network can be designed in a way that the clusters are not interfering with each other. In general the overall capacity of a cluster is determined by the access layer capacity and the mesh layer capacity (whichever is less). As pointed out in the previous section, if all the APs can be configured so that they will not interfere with each other, the access layer capacity is the sum of throughput of each AP. The mesh layer capacity is determined by the number of hops and the hop to hop throughput (explained in the following section).

Note that capacity of a cluster may or may not be the same as "single user throughput". For example, if the APs in a cluster are not interfering with each other and the mesh backhaul is not a bottleneck, the cluster capacity could be as high as the sum of single user throughput at each AP (given that there are no bandwidth restrictions configured).

2.6.13 Hop Count

The multiple hopping capability of a mesh network is introduced to increase the coverage of the network and to decrease the number of Root APs. While coverage is increased with the number of hops, the trade off is the decrease in the mesh backhaul throughput.

The multi-hopping capabilities of the wireless mesh network require that, for a packet to be relayed it must be repeated by the node; in other words, the node detects and then retransmits the packet according to the routing algorithms and rules. Any single radio transceiver in the network may only either receive or transmit at any given instant.

In the AP7161 system, there is a single radio channel for 802.11-based transmissions in each of the 2.4 GHz ISM and 5.x GHz band. As a result, for each band, all 802.11 transmissions communicate on the same channel. In other words, a single wireless mesh radio cannot send and receive at the same time.

Furthermore, a wireless mesh node can neither send nor receive data when another node is within range and is transmitting. The following point summarizes the fundamental theory of operation relating to throughput:

For radio in the AP7161 AP, the multi-hopping throughput decreases in proportion to the number of hops (1/n) when the number of hops is less than 4 (this is a characteristic of any mesh networking solution).

For example, in an AP7161 network with a single hop UDP throughput of 80 Mbps, two hop peak mesh link throughput will be roughly 40Mbps and three hops peak will be 27 Mbps. Peak is defined as all other APs are idle.

As the number of hops increases, the mesh backhaul throughput decreases accordingly. To avoid the mesh backhaul from becoming the bottle neck, a typical mesh deployment should target three mesh backhaul hops in one band (typically in 5.x GHz) and one access layer hop in another band (typically in 2.4 GHz). The following diagram shows an example of how it looks like:

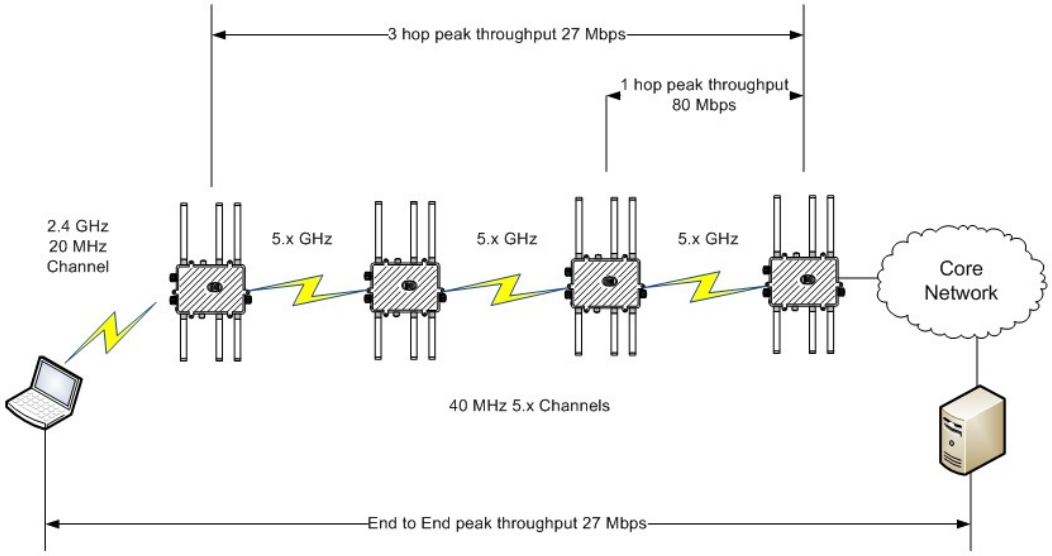


Figure 2-31

Note that when the number of hops increases to, for example, more than 5 hops, the throughput may no-longer decrease with the number of hop counts because all the APs may not be in one single collision zone and multiple APs may be able to transmit at the same time without interfering with each other. It is possible to have a mesh network of more than 5 hops but the designer would need to make sure that the delay in traffic will still meet the latency requirement of the applications that runs on top of the network.

2.6.14 Coverage, Cluster Size and AP Density

The coverage region is defined by the geographic region for which a subscriber device is able to receive an acceptable minimum service level (e.g., can send data successfully at the lowest available data rate). Coverage is synonymous with an ability for an end-user to achieve a data throughput rate at a particular

geographic locale (e.g., at a certain distance - or range - from the AP). This provides some guidelines on coverage for the wireless mesh networking technology.

Such quantitative assessments are often complex, because the RF propagation effects that contribute to the achievable signal-to-noise (e.g., the achievable data rate) are many and vary dramatically with the particular RF scenario (e.g., the RF propagation environment for a single client, including indoor or outdoor scenarios).

2.6.14.1 Cluster Coverage

Coverage of a cluster is the tradeoff between cost, throughput and hop count. One can design a lower cost network with a smaller number of APs per square mile, additional hop count, with the expectation that average user throughput and cluster capacity will be lower. The network can also be designed with a with higher AP density, less hop count, and smaller cluster coverage so that average throughput is higher. However the cost per square mile will increase.

Increasing coverage by adding additional APs may not always have the desired effect. While coverage will be increased the mesh backhaul must be sized accordingly. Additional hops may also be introduced into the network. One must take these factors into consideration otherwise the network could experience a decrease in average user throughput.

2.6.14.2 Node Density

Node Density is defined as the number of nodes per square mile. Higher node density may increase average throughput because average access layer throughput is increased. However, higher node density will not automatically lead to higher cluster capacity, if the mesh backhaul pipe remains unchanged.

Recommended node spacing is approximately .1 to .25 miles. .1 mile or less node spacing is recommended to utilize the highest data rates at the mesh layer. Keep in mind that node spacing is highly dependent on terrain. Dense urban environments with multiple of obstructions will require more nodes to achieve the desired coverage.

2.6.14.3 Number of Clients per AP

As one is designing for the network, it is important to understand that the number clients attached to the same AP will affect the access layer capacity. An increase in the number of clients in an access point may actually cause decrease in the AP throughput, due to the increase in collisions since 802.11 is a CSMA/CA protocol. This is even more significant in high data bit rate deployment scenario, for example, dual spatial stream deployment with 40MHz channel size delivering 270Mbps data rate. When the network is designed to utilize maximum data rates, the time it takes to send user data would be so short that the increase in MAC layer overhead will consume a higher percentage RF time. For example, if 80% of time is used for the MAC layer overhead such as collision, the real data rate for sending user data becomes only 54Mbps, and if we account for roughly 20% overhead in the data header and pre-ambles, the user data rate becomes only 42Mbps. Moreover, when the number of clients increases, the AP might not be able to utilize the MAC layer data aggregation feature of 802.11n, making downlink efficiency even lower.

The AP7161 can support 256 simultaneous clients. When planning a deployment an over subscription factor needs to be considered. For example an AP with a 10 to 1 oversubscription factor would support $10 \times (127) = 1{,}270$ clients.

2.6.15 Coverage Prediction

RF coverage prediction is the key element of all pre-sale planning activities. The purpose of the presale

RF coverage prediction and design is to identify the number and location of the wireless mesh networking infrastructure nodes to meet the customer coverage requirements. In general, there are two levels of design, supporting different objectives, with regard to RF coverage prediction:

- Budgetary estimates
- Broadband Planner

The budgetary design provides a rough estimate of the number and location of the mesh networking infrastructure nodes for the purpose of providing an approximate project cost. The level of detail of this design is at the discretion of the field engineer; however, this activity is not intended to produce an accurate finalized design. The detailed design is used to support a formal statement of the number of wireless mesh infrastructure nodes required.

This section provides two different approaches to support pre-sale RF coverage prediction and design. Each

approach provides a varying level of detail, complexity and accuracy. The different approaches are summarized in the following sections. In general, a combination of all techniques is recommended, where the “rules-of-thumb” and guidelines provided by past deployment experience is an essential component of all RF network designs:

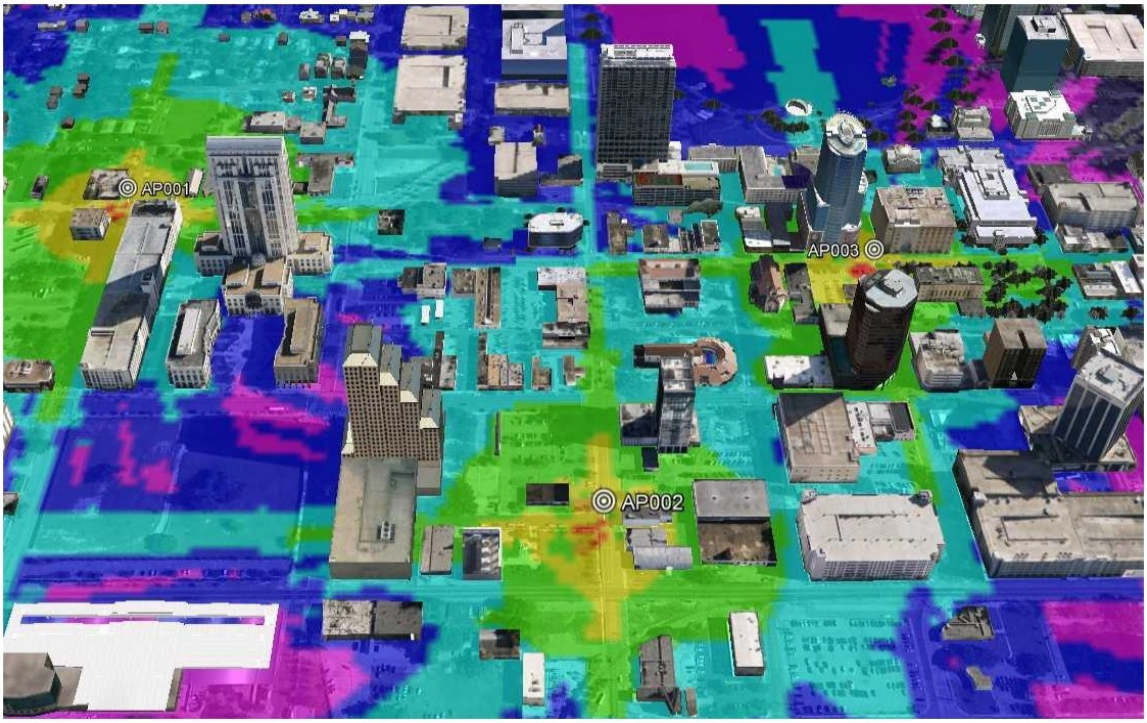
- Basic design principles; provide fundamental approach to design a wireless mesh network using basic principles, goals and guidelines (appropriate for budgetary estimation).
- On-street coverage estimation using empirical modeling; a computational method supported and calibrated with measurements.
- Detailed Ray-tracer based analysis with detail building databases; this includes a combination of computational deterministic modeling, and a mix of deterministic and statistical modeling.

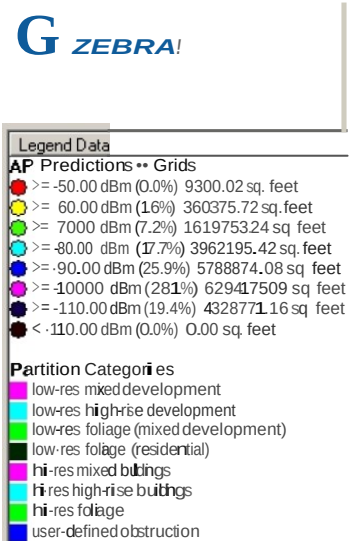
Any modeling based budgetary or detailed design technique should always be complemented by site survey and assessment activities, which include an understanding of the basic heuristic design principles. In other words, while modeling methods satisfy common RF network design goals, a site survey and site walk are essential for deployment. In addition, pre-installation coverage assessment with temporary nodes is always recommended.

It is important to consider that performing an accurate RF coverage prediction will require an investment in system planning resources and building databases. The decision to incur the cost of such an analysis is dependent on the specific customer needs, and overall project scope. The decision to employ an RF coverage prediction is dependent on the specific opportunity and requirements, and is subject to the discretion or the field and sales teams.

In general, planning for an RF deployment at the 5.x GHz band and the 2.4 GHz frequency band will require accounting for a variety of degradations that are known or unknown. When planning with the heuristic method, the impact of trees and buildings will need to be considered through a site survey and assessment of impact to coverage. Even with the computational RF coverage prediction, the impact of trees needs to be estimated; however, the tools will allow for percent-area coverage for tree density (to provide an appropriate correction factor in the calculations).

In the figure below we see the predicted covered of three APs in a downtown location. Coverage is reduced due to obstructions.





The following tables show modulation vs. signal strength.

2.4 GHz

802.11b	1	Mbps	-94	dBm
	2	Mbps	-92	dBm
	5.5	Mbps	-91	dBm
	11	Mbps	-89	dBm
802.11g	6	Mbps	-89	dBm
	9	Mbps	-89	dBm
	12	Mbps	-90	dBm
	18	Mbps	-88	dBm
	24	Mbps	-84	dBm
	36	Mbps	-82	dBm
	48	Mbps	-78	dBm
	54	Mbps	-76	dBm

802.11n	6.5	Mbps	HT20	Single	MCS	0	-89	dBm	13.5	Mbps	HT40	Single	MCS	0	-86	dBm
	13	Mbps	HT20	Single	MCS	1	-90	dBm	27	Mbps	HT40	Single	MCS	1	-85	dBm
	19.5	Mbps	HT20	Single	MCS	2	-85	dBm	40.5	Mbps	HT40	Single	MCS	2	-83	dBm
	26	Mbps	HT20	Single	MCS	3	-82	dBm	54	Mbps	HT40	Single	MCS	3	-80	dBm
	39	Mbps	HT20	Single	MCS	4	-79	dBm	81	Mbps	HT40	Single	MCS	4	-76	dBm
	52	Mbps	HT20	Single	MCS	5	-75	dBm	108	Mbps	HT40	Single	MCS	5	-72	dBm
	58.5	Mbps	HT20	Single	MCS	6	-73	dBm	121.5	Mbps	HT40	Single	MCS	6	-70	dBm
	65	Mbps	HT20	Single	MCS	7	-72	dBm	135	Mbps	HT40	Single	MCS	7	-68	dBm
	13	Mbps	HT20	Dual	MCS	8	-89	dBm	27	Mbps	HT40	Dual	MCS	8	-87	dBm
	26	Mbps	HT20	Dual	MCS	9	-89	dBm	54	Mbps	HT40	Dual	MCS	9	-86	dBm
	39	Mbps	HT20	Dual	MCS	10	-87	dBm	81	Mbps	HT40	Dual	MCS	10	-84	dBm
	52	Mbps	HT20	Dual	MCS	11	-84	dBm	108	Mbps	HT40	Dual	MCS	11	-81	dBm
	78	Mbps	HT20	Dual	MCS	12	-81	dBm	162	Mbps	HT40	Dual	MCS	12	-78	dBm
	104	Mbps	HT20	Dual	MCS	13	-76	dBm	216	Mbps	HT40	Dual	MCS	13	-73	dBm
	117	Mbps	HT20	Dual	MCS	14	-74	dBm	243	Mbps	HT40	Dual	MCS	14	-72	dBm
	130	Mbps	HT20	Dual	MCS	15	-72	dBm	270	Mbps	HT40	Dual	MCS	15	-69	dBm

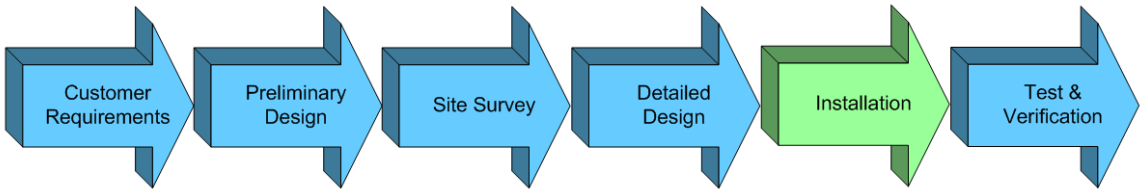
Figure 2-32

5 GHz

802.11a	6	Mbps					-92	dBm										
	9	Mbps					-92	dBm										
	12	Mbps					-91	dBm										
	18	Mbps					-89	dBm										
	24	Mbps					-85	dBm										
	36	Mbps					-82	dBm										
	48	Mbps					-77	dBm										
	54	Mbps					-76	dBm										
802.11n	6.5	Mbps	HT20	Single	MCS	0	-92	dBm	13.5	Mbps	HT40	Single	MCS	0	-88	dBm		
	13	Mbps	HT20	Single	MCS	1	-88	dBm	27	Mbps	HT40	Single	MCS	1	-85	dBm		
	19.5	Mbps	HT20	Single	MCS	2	-86	dBm	40.5	Mbps	HT40	Single	MCS	2	-83	dBm		
	26	Mbps	HT20	Single	MCS	3	-82	dBm	54	Mbps	HT40	Single	MCS	3	-79	dBm		
	39	Mbps	HT20	Single	MCS	4	-79	dBm	81	Mbps	HT40	Single	MCS	4	-76	dBm		
	52	Mbps	HT20	Single	MCS	5	-74	dBm	108	Mbps	HT40	Single	MCS	5	-71	dBm		
	58.5	Mbps	HT20	Single	MCS	6	-73	dBm	121.5	Mbps	HT40	Single	MCS	6	-69	dBm		
	65	Mbps	HT20	Single	MCS	7	-71	dBm	135	Mbps	HT40	Single	MCS	7	-68	dBm		
	13	Mbps	HT20	Dual	MCS	8	-92	dBm	27	Mbps	HT40	Dual	MCS	8	-89	dBm		
	26	Mbps	HT20	Dual	MCS	9	-90	dBm	54	Mbps	HT40	Dual	MCS	9	-86	dBm		
	39	Mbps	HT20	Dual	MCS	10	-87	dBm	81	Mbps	HT40	Dual	MCS	10	-84	dBm		
	52	Mbps	HT20	Dual	MCS	11	-84	dBm	108	Mbps	HT40	Dual	MCS	11	-81	dBm		
	78	Mbps	HT20	Dual	MCS	12	-81	dBm	162	Mbps	HT40	Dual	MCS	12	-78	dBm		
	104	Mbps	HT20	Dual	MCS	13	-76	dBm	216	Mbps	HT40	Dual	MCS	13	-73	dBm		
	117	Mbps	HT20	Dual	MCS	14	-75	dBm	243	Mbps	HT40	Dual	MCS	14	-72	dBm		
	130	Mbps	HT20	Dual	MCS	15	-73	dBm	270	Mbps	HT40	Dual	MCS	15	-70	dBm		

Figure 2-33

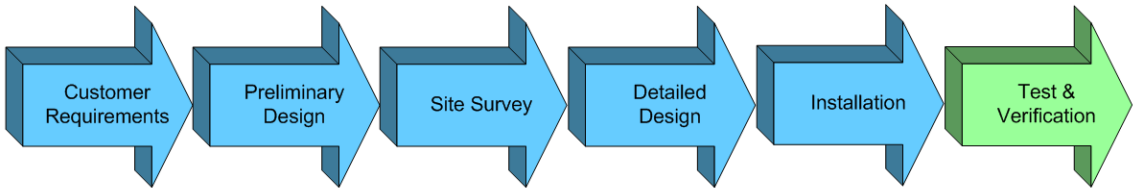
2.7 Installation



Detailed installation instructions can be found in the AP-7161 Access Point Installation Guide. However important installation notes are reiterated below.

- Make sure the device has been properly staged. If the device is to be used as a Non Root device, and it has not been configured (e.g. meshpoint), then you are essentially installing a “brick”.
- Prior to installation record the device serial number and associated MAC addresses (which can be found on the device label).
- When handling the AP7161 never hold the AP by the antenna(s).
- When attaching antennas carefully turn the antenna connector clockwise and hand tighten. The antenna should easily turn until tightened. If an antenna does not initially turn freely remove and begin again.
- When mounting ensure that the device antennas are at least 30 inches away from any metal pole / structure.
- Do not mount near overhead power lines.
- Verify that the unit and mounting asset is grounded before connecting it to a power source. This should be done by a licensed electrician.

2.8 Test and Verification



As the network is being installed it is useful to verify coverage and throughput. Coverage can be tested using by simply verifying that clients can connect in the designated coverage areas. This can be accomplished by configuring a WLAN on the deployed device and testing coverage with a laptop or handheld. However it is often useful to utilize 3rd party GPS enabled coverage tools that can create a "heat map" of the designated coverage area. Gaps in coverage can usually be addressed by adding additional devices.

2.8.1 Infrastructure

It is also beneficial to verify the infrastructure throughput capabilities. Since there are many factors that can impact throughput it is useful to know the overall maximum performance of a given link. Since the network is built outward from each Root (wired) AP throughout can be tested from each Root to each Non Root device (e.g. to each Non Root device under a given Root device).

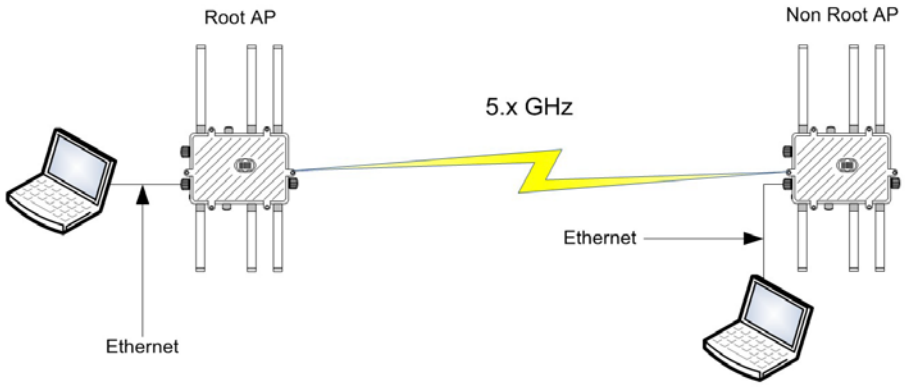


Figure 2-34

In the figure above a computer has been connected via Ethernet to the Root AP and a 1 hop Non Root AP. Tools such as *IPERF* or *IxChariot* can be used to test UDP and TCP upstream and downstream throughput. It is important to first baseline the test computers back to back to ensure that they can generate sufficient traffic. Also, tools such as IPERF can be computer dependent and may require significant "tweaking" in order to realize maximum throughput (e.g. sending multiple sessions, configuring window and buffer sizes, etc.).

Many times the path between two nodes may not have an environment capable of producing multipath thus multiple spatial streams may not be possible. This can occur in open flat environments. Increase backhaul performance can often be obtained on the backhaul radio by changing the antenna mode from default (3x3) to 2x2 or 1xall.

It's also import to verify the signal levels between the devices. Unless APs have adequate SnR (Signal to Noise Ratio) they will not be able to utilize higher data rates thus overall throughput will be limited.

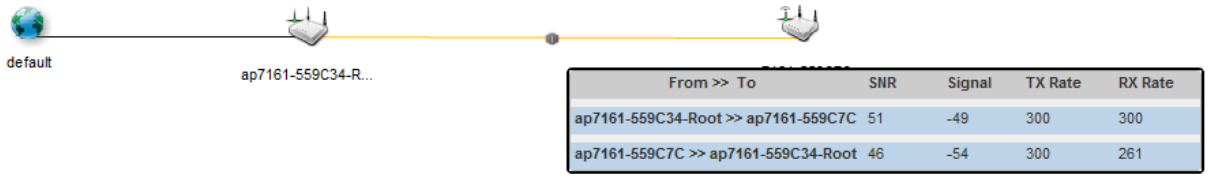


Figure 2-35

It is also useful to verify the link quality / link metric between APs. The higher the link quality the better the link (100 being the max). The lower the link metric the better the link (100-200 is considered excellent). In the example below this one hop path has a metric of 140. Note that this is information can be found in the neighbor table.

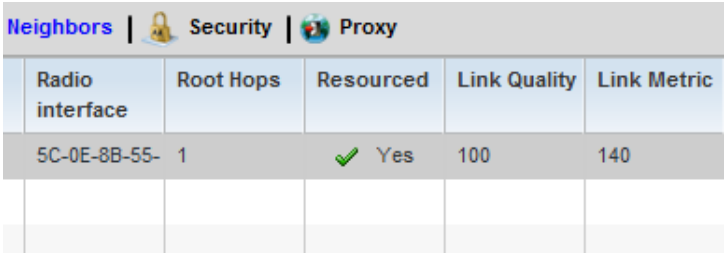


Figure 2-36

The path (or route table) in this example also displays a metric of 140 (since it is only 1 hop). If the Non Root AP happened to be 2 hops (with the first hop with a metric of 140 and the second with a metric of 200) the path table would show a total path metric of 340. Note that the path table will show a metric that is composed of all of metrics along the path from the Root to the Non Root.

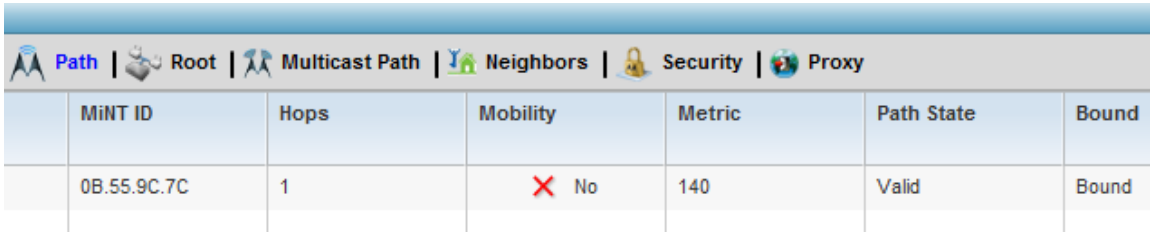


Figure 2-37

2.8.2 The Use Case

In section 2.3 understanding the customer's use case was strongly emphasized. It is important that realistic expectations are set up front to ensure that the network can support the required use case(s).

Part of the test and verification process will be to ensure that the coverage and throughput requirements of the use case are being met. During the verification process it may be necessary to add additional APs to increase the coverage area. Also, it may be necessary to add additional root APs or even reduce the number of hops to a particular AP in order to increase throughput capacity.

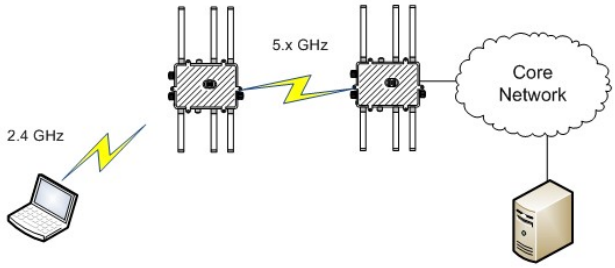


Figure 2-38

As mentioned previously, coverage areas can be verified by testing with a client device or producing a "heat map" with a 3rd party tool. Depending on the actual throughput requirements individual or multiple client tests may be necessary. If the use case contains video measured and subjective tests may also be required.

2.8.3 Network Sign Off

After the network is deployed and coverage / throughput are understood a brief report should be prepared for the customer. This report should include coverage data (e.g. individual test points, "heat maps", etc) and all throughput test data. Include photos showing a sample of the installations. This report should be included in the network sign off documents.

3 Mesh Connex™

The MCX (MeshConnex™) feature allows access points to be configured to form a mesh network. An access point with a wired connection back to the core network is referred to a mesh point root AP. Access points that are not wired into the core network are simply called mesh points. The function of the MCX software is to determine the optimum path from a mesh point, to a mesh point root. Paths between APs are created automatically by MCX. Optimum paths from mesh points to mesh point root APs are determined by the MCX algorithm. Path selection is based on metrics which are determined by device topology and the RF environment. MCX also takes advantage of the advanced rate control algorithm ORLA. The Opportunistic Radio Link Adaptation (ORLA) algorithm is a key decision-making element designed to select data rates that will provide the best throughput. Instead of using local conditions to decide whether a data rate is acceptable or not, ORLA is designed to proactively probe other rates to determine if greater throughput is available. If these other rates do provide improved throughput, ORLA intelligently adjusts rate selection to favor higher performance.

3.1 MCX Policy Settings

In order for an AP to mesh with a neighbor and form a route back to a Root AP there are several processes that must take place. After a meshpoint has been configured and mapped to a radio, beacons are used to discover potential mesh neighbors. The configured Meshid (configured in the Mesh Point Policy) must match in order for APs to become neighbors. After a neighbor relationship is formed a security relationship must be established. Security settings are also configured in the Mesh Point Policy. Security can either be configured as Open or PSK. Once this is completed path establishment can take place. In infrastructure mode this involves finding a path back to a Mesh Point Root AP (e.g. an AP with a wired connection to the core network). After a path is establish back to a Mesh Point Root device the AP must complete a binding process. The binding process simply means that the Mesh Point AP will utilize this particular Mesh Point Root to reach the core network. If a lower cost (better metric) path back to an alternative Mesh Point Root becomes available the AP could establish a path to this new Root and bind to it.

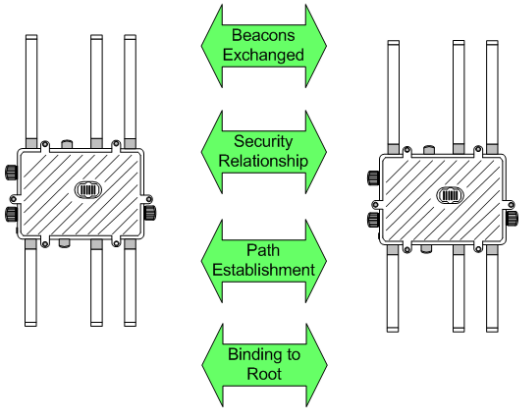


Figure 3-1

3.1.1 Mesh ID

Mesh ID is advertised in the beacon. When APs configured with mesh points exchange beacons the Mesh ID is checked. If an AP configured with a mesh point receives a beacon from another AP configured with a mesh point, and the Meshid does not match the configured the beacon is dropped. No neighbor is added in the AP's meshpoint neighbor table. Note that "mesh" beacons from neighbors are used to build the mesh point neighbor table.

3.1.2 Security

Once a neighbor is added to the meshpoint neighbor table a security relationship must be established in ordered to create a path and find a Root. There are two supported security methods support:

3.1.2.1 Open

The open security method involves a simple 2-way handshake. The exchange is as follows:

AP1 -- I want to use open security → AP2
AP2 ← Ok, use open security – AP2

3.1.2.2 PSK

The PSK security method involves multiple handshakes. The exchange is as follows:

AP1 -- I want to use psk security → AP2
AP2 ← Ok, use psk security – AP2
AP1 -- Standard 4-way from 802.11i → AP2

Once a security relationship is completed the neighbor will show up in the meshpoint security table with a Link State designated as "Enabled". At this point a path can now be created to a Mesh Point Root. For example consider a new AP that has just had a mesh point configured and has a neighbor which is 1 hop away from a mesh point root. After this AP and its immediate neighbor establish a security relationship, the new AP will send a path request through the neighbor to the mesh point root. The mesh point root will respond with a path reply. Once a path is established from the new AP, through the neighbor to the mesh point root, the new AP sends a bind request to the meshpoint root. The mesh point root will respond with a bind reply completing the process. Now the new AP is ready to route traffic from the wireless to the wired network.

3.1.3 Beacon Format

There are two beacon format choices available when configuring the mesh point policy.

Mesh Point Mode – This format is the 802.11s compliant beacon method. This is the preferred format to use except when interoperating with legacy mesh products such as MotoMesh Duo. Also note that when

using this beacon method the mesh point bss will not appear on a wireless client utility. This is preferable as the mesh bss is hidden from standard wireless clients

Access Point Mode – When this beacon format is used the AP bit is turned on in the beacon. This format should be used when interoperating with the legacy MotoMesh Duo product. Note that when this beacon format is used the mesh bss will appear on a wireless client utility.

Note that different beacon formats will not mesh.

3.1.4 Is Root

The IsRoot setting in the mesh point policy is used to denote that the AP is a mesh point root (or wired AP). Typically this setting is not checked in the global mesh point policy but rather it is set in a profile dedicated for mesh point root APs or simply as an override on an AP.

3.1.5 Neighbor Idle Timeout

The neighbor idle timeout is the amount of time that must pass in which no traffic is received from a neighbor before it is declared offline. This is typically set to a low value such as 1-2 minutes such that a non functioning neighbor will have a minimum impact on the mesh network.

3.1.6 Allowed VLANs

3.1.6.1 Local VLANs

The allowed VLANs field in the mesh point policy is used to define which VLANs are allowed to pass traffic on the mesh point. VLANs added to the allowed VLANs field are used for local VLANs (e.g. non MiNT tunneled VLANs). Thus any VLAN tagged traffic from an AP (WLAN or via Ethernet) will be allowed to cross the mesh point (non tunneled) as long as the VLAN is included in the allow VLAN field in the mesh point policy configuration.

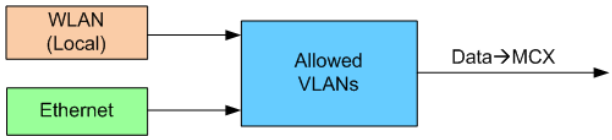


Figure 3-2

3.1.6.2 Control VLAN

The control VLAN in the mesh point policy configuration is used to facilitate Root to Root communication for handoffs. Thus this VLAN only has significance for mesh points that have the IsRoot box checked. When a device moves from under one Root to another a layer 2 update frame is sent on the control VLAN to alert the infrastructure (which includes other mesh point roots as well as core network infrastructure) that the MAC address of a mesh point root or client device has moved under a different mesh point root.

3.1.6.3 Bridged VLANs

Although not a part of the mesh point policy configuration it is important to mention bridge VLANs. A bridged VLAN is a VLAN that is tunneled over MiNT. Bridge VLANs can be configured via a device profile (or as an override) under Network→Bridge VLAN. Bridge VLANs are often used when the number of device proxies behind a single mesh point root will exceed 150 devices. When using bridged VLANs they should not be added to the allowed VLAN list in the mesh point policy configuration.

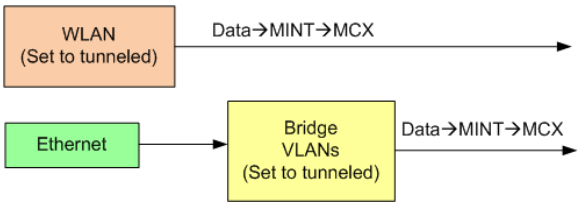


Figure 3-3

For detail information on configuring MCX please refer to the MCX How To Guide.

3.2 MCX Overrides

When configuring the MCX feature there will typically be a mix of mesh point APs and mesh point root APs (remember MPR APs are wired to the core network). **There are several configuration approaches that generate the same end result.** Consider the following example. A customer is deploying a small network with 3 mesh point root APs and 5 mesh point APs. Please refer to the "How To MeshConnex" guide for detailed instructions.

Configure two mesh point policies:
Define one mesh point policy (e.g. named MCX-RAP) with the IsRoot box checked.
Define a second identical policy (e.g. named MCX-MAP) with the IsRoot box unchecked
The customer could then create one profile for mesh point roots using MCX-RAP and an additional profile for mesh points using MCX-MAP. Each respective profile will map the appropriate mesh point policy. This method is recommended when using standalone devices.

The customer could have also configured a single mesh point policy (e.g. named MCX). The customer could also then create two profiles one for mesh point roots and one for mesh points. After mapping the mesh point policy in each profile the user would also add an additional configuration step. In the profile for mesh point root APs the user would also add the mesh point policy under **Mesh Point** in the profile configuration tree. Here the MCX policy would be selected and the IsRoot box checked. This method is recommended when using controller based networks.

Another method would be to create a single mesh point policy (with the IsRoot box unchecked) and a single AP profile. The customer would then override each mesh point root AP and add the mesh point

policy under **Mesh Point** in the device configuration tree with the IsRoot box checked. This method would require the customer to create a mesh point override on each mesh point root. This method is recommended when using virtual controller based networks.

3.2.1 Preferred Neighbor

In the device configuration tree under **Mesh Point** the user has the ability to specify a preferred neighbor. This setting can be used to bias a device using MCX mesh to utilize a specific neighbor when sending traffic. For example suppose a Non Root AP has multiple neighbors each with a path back to a Root AP. If for some reason the user determines that the chosen neighbor / path back to the Root needs to be changed a preferred neighbor can be configured. To configure a preferred neighbor the user would enter in the IFID (Interface ID) of the neighbor's mesh radio into the preferred neighbor field.

3.2.2 Preferred Root

In the device configuration tree under **Mesh Point** the user has the ability to specify a preferred Root. This setting can be used to bias a device using MCX mesh to utilize a specific Root AP. The user may configure this setting if they determine that a Non Root device should utilize a specific root. This is often used in a linear deployment to help influence Root selection. To configure a preferred Root the user would enter in the MPID of the Root's mesh radio into the preferred Root field.

3.2.3 Preferred Interface

In the device configuration tree under **Mesh Point** the user also has the ability to specify a preferred interface. This is often used when the AP is configured with MCX on multiple radios and the user would like to prioritize which radio is used for mesh.

3.3 MCX Statistics

3.3.1 Path table

The following fields are in the Path table:

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1. Note that this may change after rebooting a device if radio 2 was added first.
Destination – This field lists the Mesh Point ID of the destination for the listed path. For Root APs destinations will be other Mesh Point APs. For Non Root APs destinations will be Non Root APs as well as Root APs.
Next Hop IFID – The Next Hop Interface ID is the MAC address of the next hop's mesh radio.
Is Root – This flag indicates whether or not the AP listed in the Path table is configured as a Root AP.
MiNT ID – This is the Layer 2 MiNT ID of the AP listed in the Path table.

Hops - This field indicates the number of hops to the Root AP.
Mobility – This field indicates if mobility is enabled on the AP listed in the path table. This will always be False for a path to a Root AP.
Metric – This field indicates the path metric to the Root AP. This metric is the sum of all of the link metrics along each hop to the Root AP. The lower the number the better the metric.
Path State – This field lists the current state of the Path. Path States can be Valid, Request Timeout, Expired, In Progress, or Forward to Root. Active paths being used will be listed as Valid. Request timeout indicate there was no response to a path request. Expired indicates that a path is about to be removed. In Progress indicates that a path is being established. Forward to Root indicates that a device can be reached through the Root.
Bound – This indicates if the AP is bound to the Root AP listed in the Path table. The AP will not use the listed Root until it is bound. Bind states can be Bound, Unbound, Proxy Updated, Disfavored, or Removed.
Path Timeout – This field indicates the time in seconds remaining until the path is declared invalid. This timeout value will continue to refresh as long as the path remains valid.
Sequence – This field lists the sequence number of the Path Request.

3.3.2 Root table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Recommended – This indicates the recommended Root AP to use.
Root MPID – This is the Mesh Point ID of the listed Root AP.
Next Hop IFID – The Next Hop Interface ID is the MAC address of the next hop's mesh radio in the path back to the listed Root.
Radio Interface – This is the radio interface being used to reach the listed Root.
Bound – This indicates if the AP is bound to the Root AP listed in the Path table. The AP will not use the listed Root until it is bound. Bind states can be Bound, Unbound, Proxy Updated, Disfavored, or Removed.
Metric – This field indicates the path metric to the listed Root AP. This metric is the sum of all of the link metrics along each hop to the listed Root AP. The lower the number the better the metric.
Interface Bias – This field list the preferred interface if one has been set.
Neighbor Bias – This field lists the preferred neighbor if one has been set.
Root Bias – This field lists the preferred Root if one has been set.

3.3.3 Neighbor Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Neighbor Mesh Point ID – This is the Mesh Point ID of the listed neighbor.
Neighbor IFID – This is the interface ID of the listed neighbor.
Root MPID – This is the Mesh Point ID of the Root AP being used by the listed neighbor.
Is Root – This field indicates whether or not the listed neighbor is a Root AP.
Mobility – This field indicates if the listed neighbor is a mobile node e.g. VMM (Vehicular Mounted Modem).

Radio Interface – This field indicates the radio interface being used to reach the listed neighbor.
Hops – This field indicates the number of hops to the listed neighbor.
Resourced – This field indicates that whether or not the listed neighbor is resourced. The resourcing of a link is part of the neighbor initialization process. Note that resourced neighbors remove from the total available WLAN clients supported on a device.
Link Quality - This field lists the link quality. Link quality is a measurement of the success of packets being received by the neighbor. When no active traffic is being sent to a neighbor the Link Quality measurement is predicted via the exchange of hello packets. When there is active traffic being passed to a neighbor the Link Quality measurement is based on real MAC layer feedback. Link Quality ranges from 0 to 100 with 100 being the best link. A link quality measurement of 90-100 is considered excellent.
Link Metric – The Link Metric is a measure of performance of the link to the neighbor. The Link Metric ranges from 1 to 65,535 with lower numbers being better. However a single hop Link Metric > 1500 generally denotes a link that cannot be used. When viewed in the neighbor table the Link Metric value is a 1 hop measurement while in the Path table the Link Metric is the sum of all of the Link Metrics along the path to the Root.
Root Metric – This field lists the total Link Metric as seen by the listed neighbor to the Root AP.
Rank – This field indicates by a ranking number how important a device is. This is used in resource allocation. Ranks range from -1 to 8. -1 indicates a different mesh id or failed authentication; 0 indicates the same mesh, different root; 1 indicates the same root; 2 indicates active peer path; 3 indicates bound, or could improve via the local node; 4 indicates unbound; 5 indicates bound through local node; 6 indicates good uplink to next best root; 7 indicates good uplink to recommended root; 8 indicates current uplink to root. Please note that wireless WLAN clients will remove resources of 3 or less.

Age – This field indicates in ms the last time a beacon was heard from the listed neighbor.

3.3.4 Proxy Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Proxy Address – This field lists the MAC address that is being proxied.
Age – This field indicates the time in seconds that have elapsed since the proxy was added.
Proxy Owner – This field indicates the AP which owns the proxy device.
VLAN – This field indicates the VLAN in which the proxy is using.

3.3.5 Security table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.

Radio Interface – This field indicates the radio interface being used to reach the listed neighbor in which the security relationship has been established.
IF ID – This field indicates the BSSID of the radio of the listed security association.
Link State – This field lists the security state of the link to the listed neighbor. Links transition from the Init State, to In Progress, then either to Enabled or Failed. When a link has been successfully initialized and a security relationship has been established the link will enter the Enabled state.
Link Timeout – This field lists the time in seconds before the link must be refreshed.
Keep Alive – This field indicates whether or not a keep alive should be implemented to the listed security association. For example, if the listed neighbor is attached to another Root AP the keep alive field may not be set.

3.3.6 Multicast Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Member Address – This field lists the MPID of the AP that has the multicast subscriber attached to it.
Group Address – This field lists the multicast MAC for the multicast IP address being used.
Path Timeout – This field lists in ms how long to keep the multicast subscription active. Note that a -1 indicates "forever".

3.4 Virtual Controller

The virtual controller feature in WiNG allows for a single AP to provide functions normally associated with a wireless controller. This feature will allow an AP to adopt other APs enabling it to provide configuration updates, automatic firmware updates, smart RF, and statistics collection. For customers that have a single location or businesses owned by a parent company but are individually managed virtual controller mode is often used.

3.4.1 Limits

Single profile – Unlike a controller that supports multiple device profiles an AP using the virtual controller feature only supports a single profile. When configuring a virtual controller network using MCX the single profile can be configured several different ways.

The global MCX policy can be configured to include the "Is Root " option checked. Then this policy can be assigned to a radio(s) within the device protocol. Also within this policy, under **Mesh Point** the global MCX policy should be added with the IsRoot true and the Monitor Primary Port Link button checked. By doing so devices that are not wired to the network will become Non Root devices when a wired connection is not connected.

The user can also configure the global MCX policy with the IsRoot option unchecked. This policy would then be assigned to a radio(s) in the single profile. Next the user would use a device override to add a meshpoint in the device configuration tree under **Mesh Point** and select the IsRoot option.

Single RF domain – Only a single RF domain is supported when using the virtual controller feature.
Tunneled VLANs not supported – The use of tunneled VLANs is not supported when using the virtual controller feature.
Managed APs must be same model – When using the virtual controller feature only like model devices are supported. For example, when using the virtual controller feature on the AP7161 only AP7161s will be adopted.
Maximum 24 APs – When using the virtual controller feature the network must not exceed 24 APs.

For additional information please see the MCX in Virtual Controller How To Guide.

3.5 WLANs, VLANs, and MCX

3.5.1 Local VLANs

When configuring a WLAN the user has the option to make the VLAN local. When using this option WLAN traffic is bridged locally (i.e. this method is sometimes referred to as using independent VLANs). VLAN tagged traffic coming into the Root AP is forwarded to the core network and switched accordingly. In this method the wireless controller is removed from the data path. However the wireless switch can still be used to manage the network. Note that when using this VLAN method VLAN tagged WLAN traffic is encapsulated in MCX and forwarded through the mesh to the Root AP. The mesh Root AP removes the MCX header and forwards the VLAN tagged data out the GE1 port (assuming GE1 is configured as a trunk which includes the VLAN configured for the WLAN). The VLAN tagged data is then forwarded by the wired network. It is important to note that when configuring the global MCX policy that all local VLANs that have been assigned to WLANs be added to the Allowed VLANs list. Any tunneled VLANs should not be included in the allowed VLANs lists.

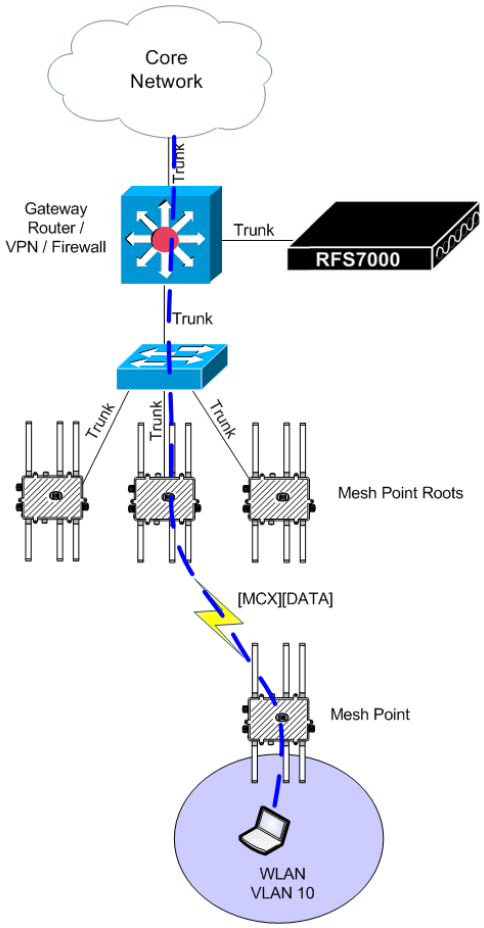


Figure 3-4

3.5.2 Tunneled VLANs

When the user is configuring a WLAN they also have the option to make the VLAN tunneled. When using this option traffic is tunneled over MiNT to the controller (i.e. extended VLANs). VLAN tagged traffic coming into the Root AP is forwarded to the wireless controller. From there the traffic is forwarded to the core network accordingly. Note that when using this VLAN method VLAN tagged WLAN traffic is encapsulated into MiNT, then MCX, which is then forwarded through the mesh towards the Root AP. The mesh Root AP removes the MCX header and forwards the MiNT encapsulated VLAN tagged data to the wireless controller via the MiNT VLAN. From there the wireless controller removes the MiNT VLAN / header and forwards the VLAN tagged data to the wired network. It is important to note that when configuring the global MCX policy that all tunneled VLANs that have been assigned to WLANs should NOT be added to the Allowed VLANs list. Also, if there is a device added to an Ethernet port of a Mesh Point AP (e.g. a camera) that is VLAN tagged and needs to be tunneled then a bridge VLAN should be added to the device and marked as tunneled.

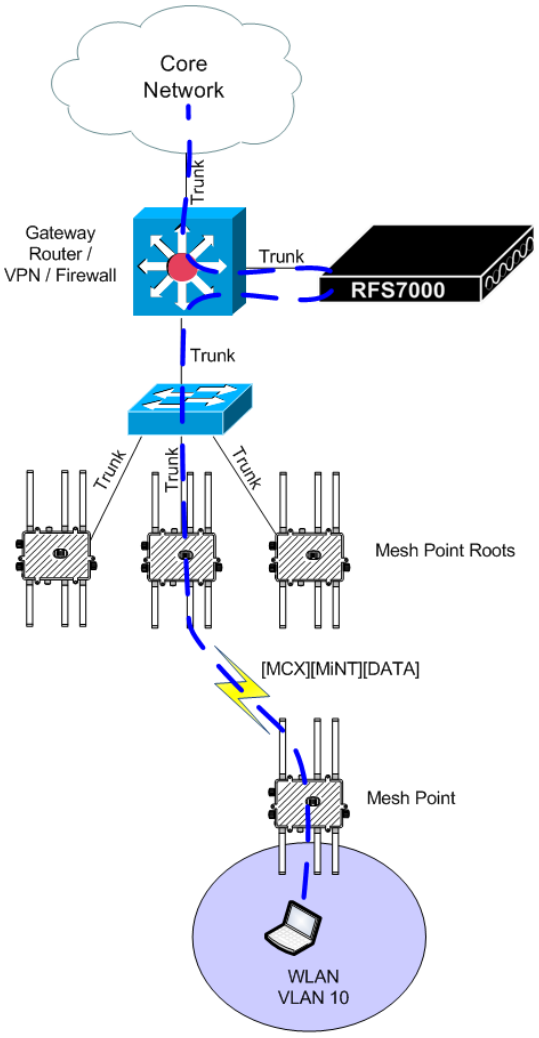


Figure 3-5

3.6 IP Planning

When configuring a 7161 network multiple VLANs / IP subnets are often used to separate WLAN / Ethernet traffic. 7161s can also be configured with a multiple VLAN interfaces each of which can be used to reach the AP over IP (e.g. accessing the individual AP's webpage). When assigning an IP subnet to a VLAN, IP ranges defined in RFC1918 should be used. The actual choice of private internet IP addresses depends on the expected size of the deployment and the existing configuration of the customer's network. Note that IP addresses assigned to the AP themselves are not required in a controller based network using MiNT layer 2 traffic.

Private Network IP Ranges

Subnet	Size
10.0.0.0/8 (10.255.255.255)	16,777,214 hosts
172.16.0.0/12 (172.31.255.255)	1,048,574 hosts
192.168.0.0/16 (192.168.255.255)	65,534 hosts

Figure 3-6

There is another consideration when planning IP subnets. A VLAN corresponds to a broadcast domain and it is recommended that the size of any one IP subnet be limited between 250-500 devices. If it is anticipated that the number of IP addresses required on any one VLAN will exceed this number then another VLAN / IP Subnet should be added. The subnetting example listed here shows how one might obtain a subnet with 500 hosts using private network addresses.

Subnet ID	Subnet Mask	Mask Bits	Max Hosts	Subnet Host Address Range	Subnet Broadcast Address
10.0.0.0	255.255.254.0	23	510	10.0.0.0 - 10.0.1.254	10.0.1.255
10.0.2.0	255.255.254.0	23	510	10.0.2.1-10.0.3.254	10.0.3.255
10.0.4.0	255.255.254.0	23	510	10.0.4.1 - 10.0.5.254	10.0.5.255
10.0.6.0	255.255.254.0	23	510	10.0.6.1 - 10.0.7.254	10.0.7.255
….	….	….	….	….	….
10.255.254.0	255.255.254.0	23	510	10.255.254.1 - 10.255.255.254	10.255.255.255

Figure 3-7

3.6.1 Addressing

3.6.1.1 DHCP

Dynamic Host Configuration Protocol (DHCP) enables the centralized management and automation of the assignment of IP addresses for both 7161 APs and WLAN clients. The primary advantage of network DHCP is the ease of management and configuration of IP addresses. For example consider a client WLAN. WLAN clients can change very frequency and managing static IP addresses can be very tedious. By using DHCP, WLAN clients will be automatically assigned an IP addresses. When configuring a WLAN select a VLAN that has been configured for DHCP.

DHCP services can be provided by an RFS wireless switch or even by the APs themselves. For large 7161 networks controller based DHCP or external DHCP sources should be used. In simple single AP “hotspot” applications DHCP services can be provided by the AP.

3.6.1.2 Static

Static IP addressing is often used for addressing wireless assets that are permanent and fixed. It is often more practical to assign an IP address that will not change to these types of devices. This is especially true when using applications that require the user to manually enter in the IP address of the device in which the application must access. Note that it is often good practice to still enable DHCP on the VLAN / IP subnet being used. That way a misconfigured device may still receive an IP address. The user must make sure that the configure DHCP range does not overlap the static IP range in the subnet.