



Control4 Zigbee PRO

BEST PRACTICES
AND DESIGN GUIDE



Contents

Introduction	4
Control4 Zigbee PRO	4
Mesh networks	5
Zigbee meshes are reliable	6
Zigbee device types	7
Nodes	7
Router nodes	7
End nodes	7
Mesh controller	7
Each Zigbee mesh is secured with a unique key	8
Connecting devices to the Zigbee mesh	9
Firmware updates and network slowdowns	9
Zigbee design guidelines	10
1. Do not put a mesh controller in a rack	11
2. Use a secondary controller as a mesh controller	11
3. The mesh controller should be central to the mesh	12
4. Keep the mesh controller away from WiFi	13
5. Limit a mesh to 70 nodes	13
Planning the mesh configuration	14
How Zigbee devices route and reroute	14
Radio and relationships	15
Radio range for Zigbee devices	15
Wireless interference to Zigbee signals	16
Routing limitations for end nodes	17
Choosing a Zigbee channel	17
Default channel selection	17
Planning for a good Zigbee channel	18
Scanning for an optimal channel	19
Advanced configurations	19
Scaling your mesh design for large projects	19
Multiple meshes	20
Scaling	21
Limitations of the “mesh controller” approach	21

Multiple ZAP use case 1: Roaming remotes.....23

Multiple ZAP use case 2: Large lighting scenes23

Terms and definitions.....24

Legal notices..... 25

Introduction

This guide is for Control4 Dealers and their certified technicians. It outlines important Zigbee concepts and recommendations to help you design and implement durable Control4 systems with fast, reliable Zigbee networks.

NOTE

Recommendations in this document are for systems with EA and CA controllers running Control4 OS 2.10 or newer and are subject to change with the release of new Control4 hardware or software.

PRO TIP

For training on IP networking principles, enroll in the PCNA (Pakedge Certified Network Administrator) course. Read more about it at pkdge.co/pcna-faq.

Control4 Zigbee PRO

Zigbee is a 2.4 GHz wireless communication technology used for reliable, low-bandwidth networks. Control4 uses a version of Zigbee called *Control4 Zigbee PRO* that improves security so that it can be used in sophisticated smart-home systems. Throughout this document, “Zigbee” refers to Control4 Zigbee PRO, not the original version of Zigbee.

Mesh networks

Zigbee devices link together to create a mesh network.

How devices link together on a network is called a *topology*. Since many are already familiar with WiFi networks, it may help to compare Zigbee's mesh topology with WiFi's star topology.

WiFi uses a *star topology* where each device can only communicate directly with the WiFi access point. These networks, which are often high bandwidth but are limited in range, are not typically self-healing.

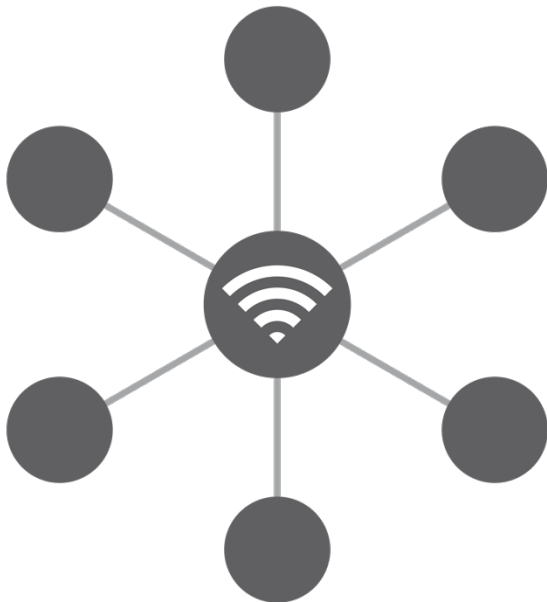
Zigbee networks use a *mesh topology* where all devices ("nodes") can communicate with each other to form a wireless *mesh network*. A mesh network differs from a WiFi network because devices ("nodes") in a mesh network can communicate directly with any other device in range, while WiFi devices can only communicate directly with a wireless access point.

Topology: The path that data takes to travel around the network.

Star topology: Each device talks directly to the wireless access point.

Mesh topology: All devices ("nodes") can talk to each other to relay messages to and from the mesh controller.

Star network topology (WiFi)



Mesh network topology (Zigbee)



Zigbee meshes are reliable

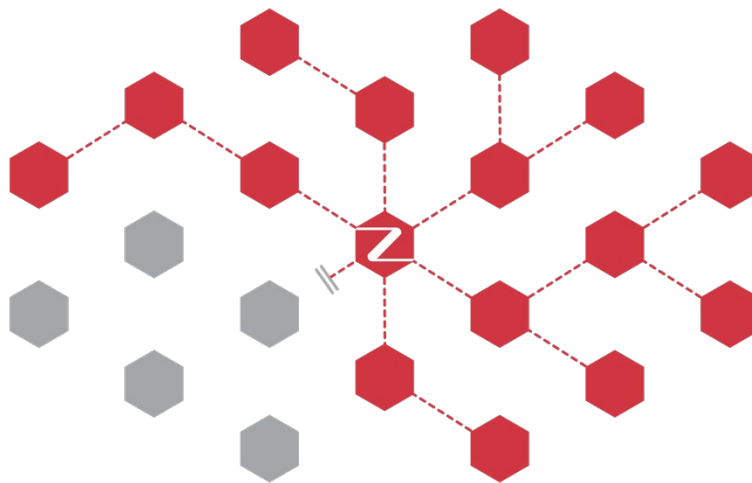
A Zigbee network is self-organizing and self-repairing. Devices can communicate over numerous paths and regularly optimize their connections to other devices, enabling the mesh to automatically recover from wireless interference or broken links.

Zigbee networks can also cover large areas as messages are relayed from one device to another, eventually communicating with more distant devices on the mesh.

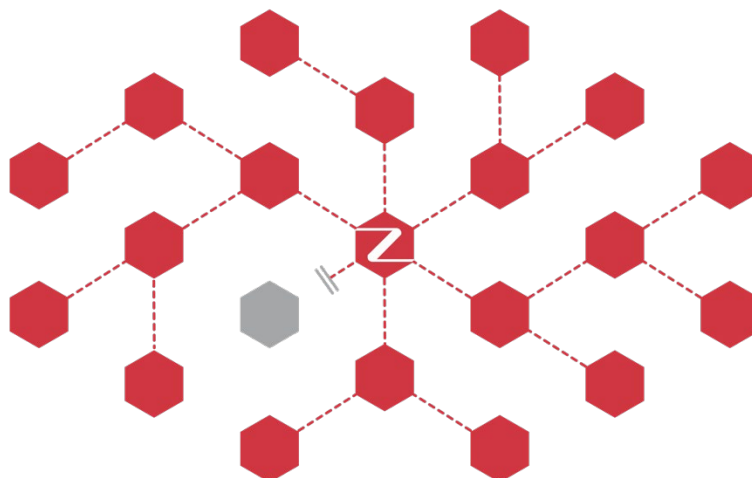
falling offline—When a device disconnects from the network, usually due to a weak signal or power failure.

re-routing—Each device talks directly to the wireless access point.

One disconnect potentially becomes many
When a device disconnects from the network (“falls offline”),
it can no longer repeat messages to other devices



Re-routing saves the day
Zigbee devices will re-route to stay online and available



Zigbee device types

Nodes

Zigbee devices are called *nodes* and are categorized as either *router nodes*, *end nodes*, or a *mesh controller*. Zigbee nodes that communicate with each other form a *Zigbee mesh network*.

Router nodes

Router nodes are always-on Zigbee devices that can relay messages to and from other devices on the network. They extend the range of the network by enabling distant devices to communicate with the mesh controller. Router nodes must be constantly powered, so battery-powered devices are never router nodes. An example of a router node is a Control4 Wireless Dimmer for controlling lights.



Router node icon used in diagrams include this symbol



Examples of router nodes include

End nodes

End nodes communicate with a router node or a mesh controller but do not relay messages from one device to another. They do not extend the reach of the mesh network or make the network more reliable. Battery-powered devices conserve power by communicating only periodically, unlike an always-on routing node. An example of an end node is the SR-260 System Remote Control.



End node icon used in diagrams include this symbol



Examples of end nodes

Mesh controller

Each mesh has one mesh controller that connects the mesh devices to the Control4 platform. The mesh controller is always on a Control4 controller. The two processes that make up the mesh controller are *Zserver* and *ZAP*. A project may include multiple mesh controllers, but each mesh can have only one mesh controller.



Mesh controller icon used in diagrams

Each Zigbee mesh is secured with a unique key

When you first create a mesh network on a controller, the Control4 system configures and enables the software processes (ZServer and ZAP) to run on the mesh controller. The process of configuring a Zigbee network in Composer Pro is explained in the *Composer Pro User Guide* at ctrl4.co/cpro-ug.

Control4 Zigbee PRO has strong security. When created, the mesh controller generates a unique security key to encrypt the network's communications. That security key is shared with devices when they are identified to the project. The key is also stored in the project and in any subsequent project backup.

NOTE

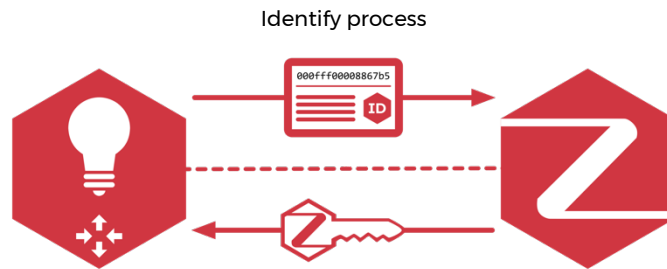
If you ever need to reset a controller, the Zigbee security key is stored in the Control4 project backup and gets restored when the project is restored.

PRO TIP

Do *not* copy a Control4 project file with Zigbee security key to other controllers or projects. Loading the project to another controller also loads the same security key, which can cause multiple Zigbee mesh networks to conflict with each other. This conflict can cause all devices to get rejected from one or both active meshes.

Connecting devices to the Zigbee mesh

When you identify a Zigbee device in Composer, the device's unique (MAC) address is stored in the project, and the mesh's Zigbee security key is shared with the Zigbee device. (For help with the process of identifying a Zigbee device in Composer Pro, see the *Composer Pro User Guide* at ctrl4.co/cpro-ug.) The mesh controller can now communicate with the Zigbee device, and the device now has the security key to communicate on the mesh.



The Zigbee device sends its ID to the mesh controller, and the mesh controller sends the mesh's security key to the device.

PRO TIP

The security key gets shared only when you identify the Zigbee device to the Control4 project. At any other time, the mesh controller does not allow any new devices to join, and all communications are encrypted by the Zigbee security key.

Firmware updates and network slowdowns

Shortly after a Zigbee device is identified, the mesh controller automatically performs firmware updates on devices that need them. While a firmware update is in progress, Zigbee mesh network communications will slow down, and the Zigbee device may reboot (which may result in light fixtures turning off and on). Because firmware updates are bandwidth intensive, the system updates no more than three devices at a time.

Zigbee design guidelines

Zigbee network designs vary based on the specific requirements unique to each location, but most successful Zigbee networks follow these five major guidelines. These guidelines should also be used for troubleshooting and optimizing existing Zigbee networks.

You can download a printable version of this infographic at ctrl4.co/zigbee-infographic.



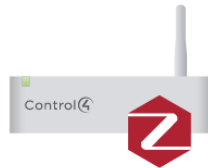
Rule of Thumb



Never put a mesh controller in a rack. Racks block wireless signals.



2nd Finger



Use secondary controllers for mesh controllers.



Middle Finger



Put the mesh controller central to the devices in each mesh.



Ring Finger



Never locate WiFi access points within a 5 meter (15 feet) ring around a mesh controller.



Small Finger



Limit a mesh to fewer than 70 devices. For more than 70, setup additional mesh controllers.

1. Do not put a mesh controller in a rack

An equipment rack encloses the mesh controller in metal, creating a barrier (like a Faraday cage) to Zigbee signals. Other electronic devices in the rack cause interference and severely limit Zigbee signal strength. Also, the equipment room is seldom centrally located to the rest of the Zigbee mesh and can have radio obstructions such as high-voltage wiring, metal plumbing, and concrete walls.



PRO TIP

If the mesh controller absolutely *must* be placed in the rack, use a Control4 3-meter Wireless Antenna Kit (C4-AK-3M) to extend the Zigbee antenna outside of the rack, but be aware of other radio obstructions.

2. Use a secondary controller as a mesh controller

When possible, use a secondary controller as the mesh controller. Select a secondary controller that is not in an equipment rack. Especially consider moving the mesh controller to a secondary controller if the secondary controller is in a more centrally located area to the rest of the Zigbee devices.

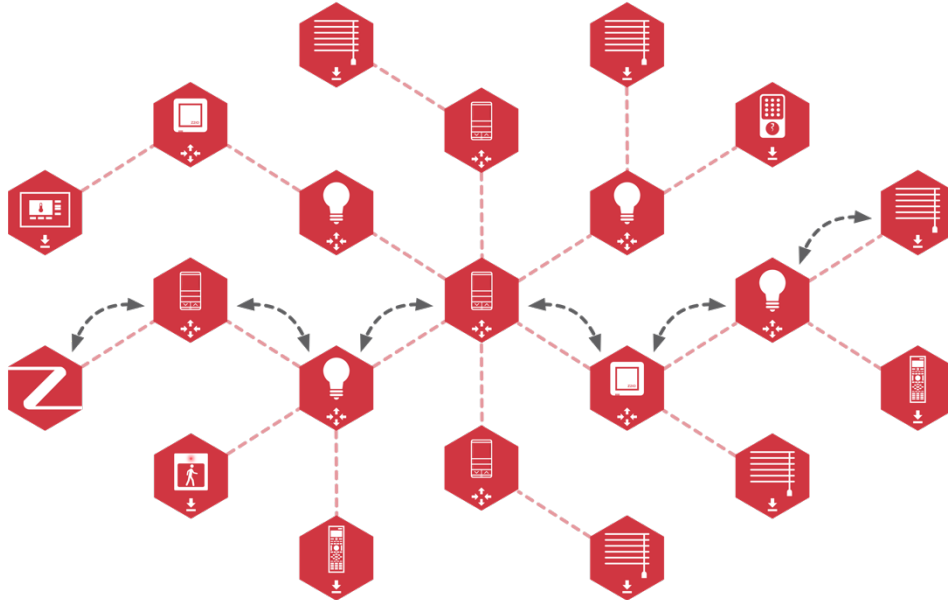


Also, it's a common misconception that the mesh controller should always be configured on the primary controller. Moving the mesh controller configuration to a secondary controller can free up processing power to run Director on the primary controller but will add some networking latency between Director and the mesh controller. Make sure that if your mesh controller is on a secondary controller, the controller is hardwired to a reliable Ethernet network.

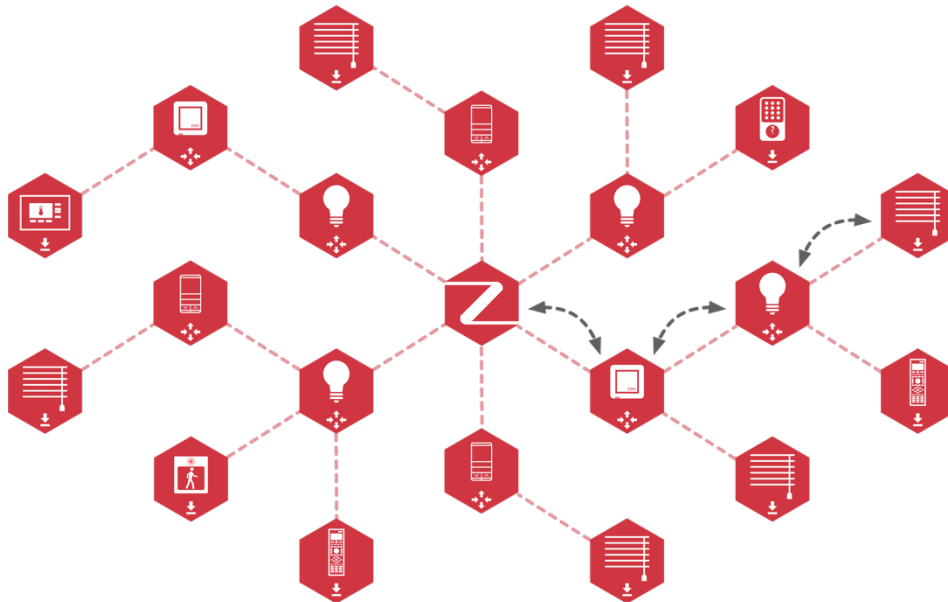
3. The mesh controller should be central to the mesh

Locate the mesh controller centrally among the mesh devices. When the controller is not centrally located, the mesh may run more slowly because some devices have more “hops” (whenever a signal is received and re-sent from a device) back to the mesh controller. Also, the mesh may not be as resilient, because there are fewer devices to relay messages back to the mesh controller.

When the mesh controller is not located centrally to the other devices in the mesh network, it causes latency through additional hops.



When the mesh controller is centrally located, performance improves because there are fewer hops to each device in the mesh.



4. Keep the mesh controller away from WiFi

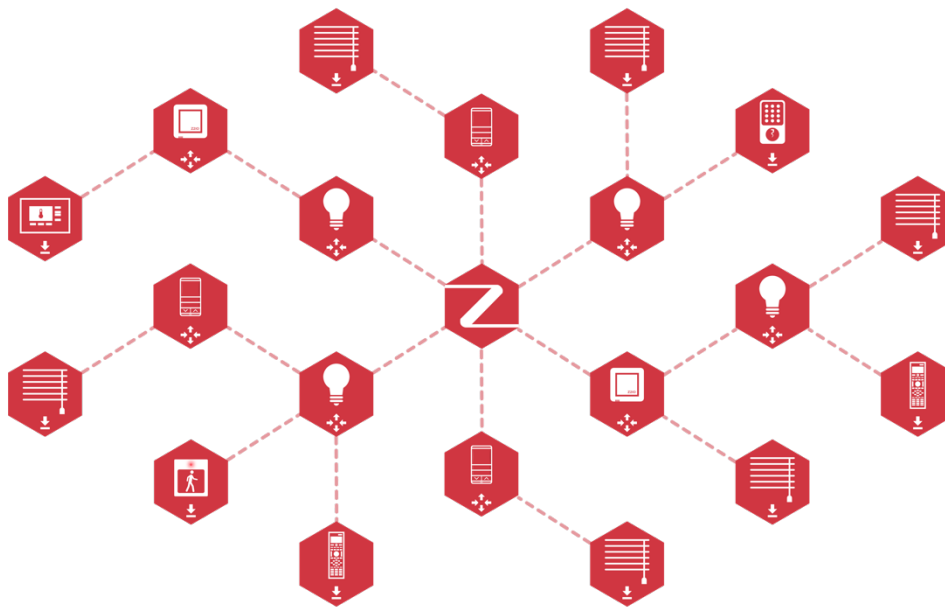
A WiFi router or access point co-located with a mesh controller can overpower *all* Zigbee communication to that controller, even if the channels are not overlapping. Always move the WiFi router or access point at least 5 meters (15 feet) away from the mesh controller.



At least 5 meters (15 feet) apart

5. Limit a mesh to 70 nodes

Limit each mesh to 70 or fewer nodes. Performance degrades when too many devices are connected. If you have more devices, configure another mesh controller and distribute devices between them as evenly as possible.



Limit mesh networks to 70 nodes or fewer

Planning the mesh configuration

Now that you understand a few basics about the Zigbee mesh and know the most important design guidelines, you can use that knowledge to design your Zigbee network.

Knowing how Zigbee devices route (and reroute when needed) and how obstructions limit your Zigbee signal strength will help you know where to put Zigbee devices.

How Zigbee devices route and reroute

Zigbee devices should have multiple possible paths to the mesh controller. Make sure that the Zigbee devices are positioned so that they don't all communicate through a single route back to the mesh controller.

Controller is *not* central

A large group of devices all communicating to one router node creates a communication bottleneck. If that router node stops working, then all of the other devices that route through it will go offline. Here, the node closest to the controller lost its connection, leaving the rest of the devices without communication.



Controller *is* central

Locating the mesh controller in a central location creates greater routing flexibility. Here, multiple routing nodes are connected to the mesh controller, so if one communication route fails, the devices can re-route and maintain communications.



PRO TIP

To ensure each Zigbee device is within the range of a routing node, always identify devices where they will be installed, and start first with identifying the devices closest to the mesh controller. If the device has trouble being identified to the project, it may indicate it's not close enough to a routing node.

Radio and relationships

Radio range for Zigbee devices

Radio signals weaken rapidly over distance and when moving through or reflecting off dense objects. This weakening is called “attenuation.” Radio signals can also degrade from radio signals or electronic “noise” that interferes with the mesh controller’s availability to send messages. Although a signal is hampered through attenuation, it can still work but will lower the performance of the mesh network. The following recommendations will help you achieve optimal signal strength and clarity for your mesh network, mitigating potential communication problems as you build out the project.

Distance

Most environments allow only **5 to 9 meters (15 to 30 feet)** between devices for optimal signal strength. This can be as little as 2 to 3 meters (6 to 9 feet), depending on construction materials or interference between your devices, or it could be a much longer range, in open air, without any interference.

Recommended maximum device range

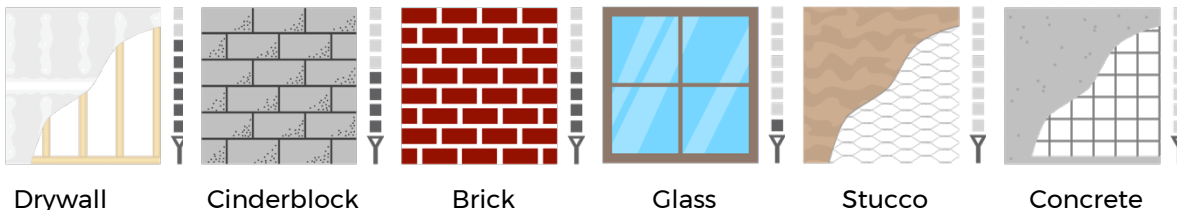


5 meters (15 feet)

While Zigbee messages may successfully reach nodes at much longer ranges than described above, the device may retry sending the messages several times, which can cause latency and reduce overall mesh performance.

Physical obstructions to Zigbee signals

Construction materials obstruct radio signals to varying degrees. Concrete floors, steel-reinforced floors, ceilings, walls, elevator shafts, masonry, rock, radiant floors, cinder block, chicken wire-reinforced materials such as Venetian plaster, stucco, and similar building materials degrade or attenuate wireless signals. Add controllers and multiple meshes or extra router nodes into projects where these signal barriers exist.



Drywall

Cinderblock

Brick

Glass

Stucco

Concrete

In addition to construction materials in the walls and floor, items in the room can also reduce wireless range. Some examples of “Zigbee killers” include these usual suspects:

- Kitchen appliances and similar items with a lot of metal and insulation, such as refrigerators, freezers, and washers and dryers
- Large fish tanks, hot water tanks, and other water reservoirs
- Items that use signal-limiting materials, such as a concrete chimneys or elevator shafts
- People, when congregating in large numbers



Wireless interference to Zigbee signals

Third-party devices that transmit on the same wireless frequency (channel) as the Zigbee mesh—or on all channels—can impact Zigbee performance. Other devices that don't even use wireless communications, like a microwave, can also impact performance. To learn how to choose an effective, relatively interference-free Zigbee channel, see “Choosing a Zigbee channel” on page 17.

Other household electronics can also impact the performance of the Zigbee mesh network:

- Bluetooth
- 2.4 GHz cordless phones
- WiFi networks
- Wireless speakers
- Baby monitors

Zigbee communicates on the 2.4 GHz band and shares those frequencies with many other home electronics. These other devices cause interference when they transmit on the same channel as the Zigbee mesh. The mesh controller won't attempt to send any communications when a high amount of interference is present—it will wait for the channel to be clear which may introduce significant latency into the network.

PRO TIP

To avoid cordless phone interference on 2.4 GHz, consider upgrading your client's cordless phone system to a 5.8 GHz or DECT 6.0 type.

IMPORTANT

While construction materials, furnishings, and even living occupants can act as radio *obstructions* that attenuate Zigbee signals, there are also devices that actively emit radio interference.

For example, a WiFi router or wireless access point co-located with a mesh controller can block *all* Zigbee communication from that controller, even if the channels are far apart. To resolve this, move the WiFi router or AP at least 5 meters (15 feet) away from the mesh controller.

Routing limitations for end nodes

Each routing node (or controller) can have a limited number of end nodes connected at once:

- Control4 controllers and the Z2IO support up to **32** end nodes.
- Wireless lighting devices (for example, configurable keypads, switches, and dimmers in Decora and square configurations) support up to **16** end nodes.
- Legacy (pre-2013) Zigbee PRO devices (for example, 6-Button Keypad or Wireless Dimmer) support up to **six** end nodes.

Note: These restrictions only apply to *end nodes*, for example a system remote control, not other routing nodes that communicate through the routing node.

A mesh with too many end nodes creates communication problems. End nodes get “orphaned” because there is not a router node or mesh controller in range to communicate with. In contrast, if you have many router nodes, they can communicate with any device in range.

IMPORTANT

Don't design your Zigbee nodes with too many end nodes (remotes, thermostats, and other battery-operated devices).

For example, if you have 33 or more end nodes in a project with only a mesh controller and no other routing nodes, only 32 of those devices can be connected to the mesh controller at a time. Add routing nodes throughout the system to help the end nodes connect and communicate more effectively.

Choosing a Zigbee channel

Default channel selection

Zigbee channels, along with many other wireless devices that use WiFi or Bluetooth, use the 2.4 GHz wireless band. When you configure a Zigbee mesh in Composer, the mesh controller scans for and selects the least-used Zigbee channel.

PRO TIP

This channel selection happens only once, when you first set up the mesh. The controller does not continually check for a better channel.

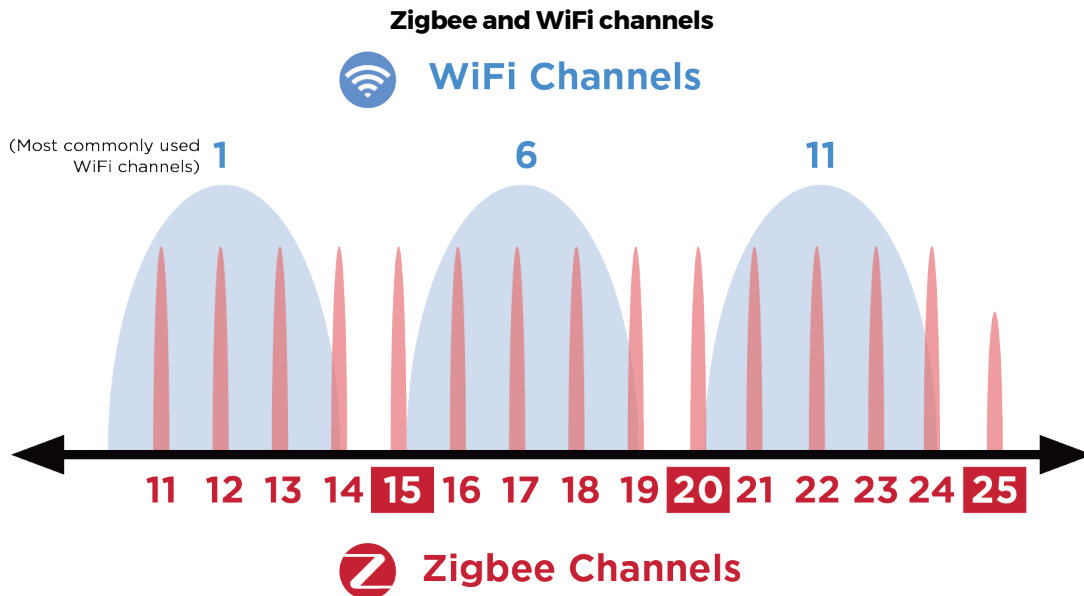
PRO TIP

Never settle for the default channel selection. Always assign a mesh's channel deliberately, and plan your Zigbee channel to be clear of WiFi and other Zigbee channels. To learn how to assign a Zigbee channel in a mesh, see the *Composer Pro User Guide* at ctrl4.co/cpro-ug.

Planning for a good Zigbee channel

The Zigbee standard defines 15 channels, all within the 2.4 GHz radio band. Because WiFi shares this band with Zigbee and can easily interfere with it, you must plan Zigbee channels to work alongside WiFi channels without interference.

Zigbee channels are numbered 11-25, but they overlap many of the same frequencies as WiFi channels 1-11. Zigbee channels are narrow (2 MHz wide), while WiFi channels are wide (22 MHz), so a single WiFi channel can interfere with multiple Zigbee channels.

**PRO TIP**

To select a Zigbee channel that does not overlap with WiFi, try channel 15, 20, or 25. These Zigbee channels avoid the most common WiFi channels (1, 6, 11). Also note that channel 25 in the US has lower transmission power per FCC requirements.

Scanning for an optimal channel

Third-party devices can cause intermittent wireless interference. This interference may not always be present because the interfering signals might be from portable devices that are not always in the home or devices that are not always transmitting. If the channel was set during intermittent down time, Zigbee performance will suffer when that interference source becomes active. Find sources of interference by **performing a site scan for 24 hours** with a 2.4 GHz spectrum analyzer. A shorter scan may not always find the cause of intermittent interference.

PRO TIP

MetaGeek Wi-Spy is a recommended wireless spectrum analyzer, and it can be purchased on the Online Portal (<https://dealer.control4.com/products/653>).

Advanced configurations

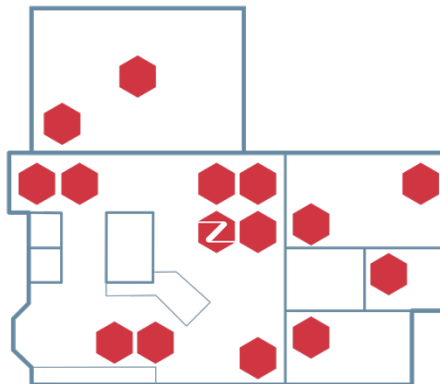
Scaling your mesh design for large projects

Zigbee scales from the smallest to the largest of projects. The scale of a project should guide the mesh network design.

The two recommended deployments for a Zigbee mesh are:

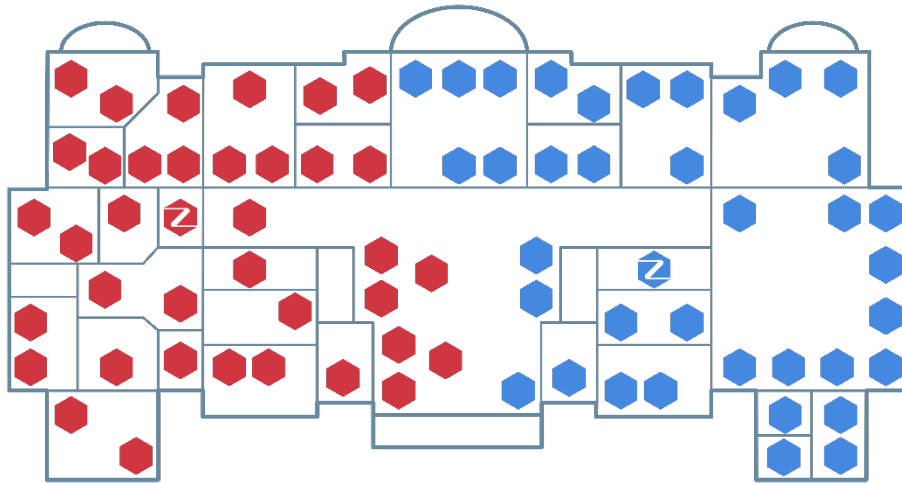
- **Single** mesh controller forming **one** mesh—up to 70 devices, all located within a reasonable range.
- **Multiple** mesh controllers forming **separate** meshes—for more than 70 total devices or when devices are spread over a wide area.

Single mesh controller example



- Few devices
- Mesh controller located central to nodes

Multiple mesh controllers example



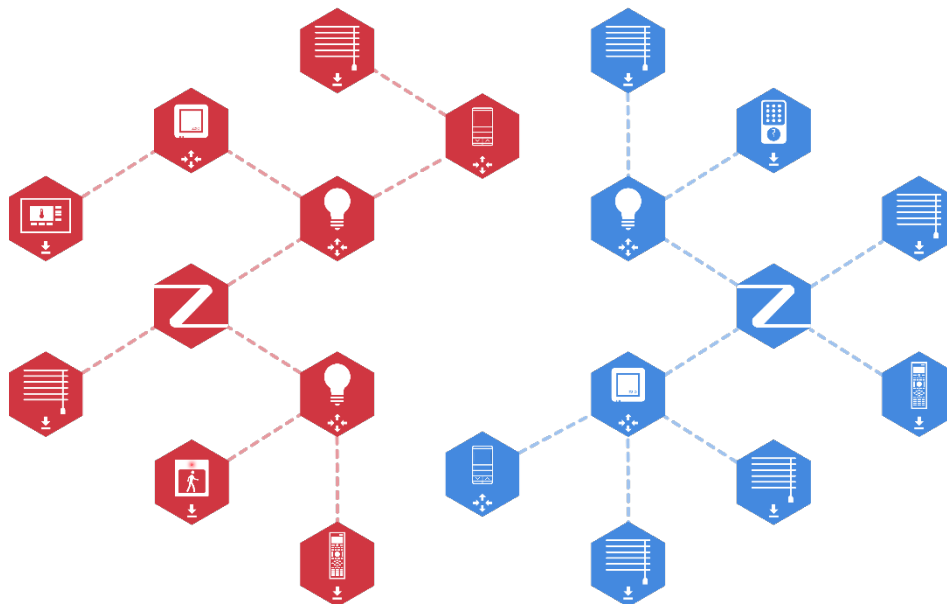
- Many devices
- Multiple mesh controllers
- Each mesh controller located central to nodes

Multiple meshes

If a project with one mesh controller has more than 70 nodes, split the project into two or more meshes.

Multiple meshes example

Two independent meshes, each having its own mesh controller



Scaling

Control4 has successfully tested the following configurations for scalability:

- **8** mesh controllers with **70** Zigbee devices/nodes per mesh
- **16** mesh controllers with **50** Zigbee devices/nodes per mesh
- **20** mesh controllers with **25** Zigbee devices/nodes per mesh

Find information about how to create multiple Zigbee mesh networks in *Composer Pro User Guide* (ctrl4.co/cpro-ug) and in the Knowledgebase (kb.control4.com).

Limitations of the “mesh controller” approach

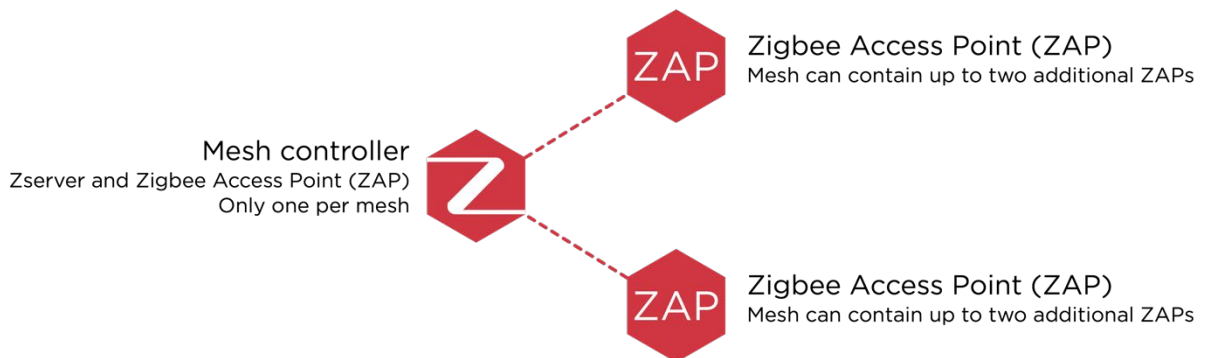
You can also scale the Zigbee mesh by configuring additional Zigbee access points (ZAPs) in each mesh network that already has a mesh controller. Note that this is different from just creating multiple meshes. For help with enabling an additional ZAP in Composer Pro, see the Composer Pro User Guide at ctrl4.co/cpro-ug.

Some Zigbee installations require configurations that are more complicated than using one or multiple mesh controllers in a project (see the use cases below—roaming remotes and large lighting scenes). Before discussing these methods, it’s important to know the meaning of some key terms:

Zigbee mesh controller—Manages Zigbee communications. Each mesh controller runs two software processes: ZServer and ZAP (Zigbee Access Point). A controller with both ZServer and ZAP running on it is a mesh controller. A mesh can have only one mesh controller.

ZAP (Zigbee Access Point)—A software process that runs on a Control4 controller and controls the Zigbee radio. A ZAP communicates with Zigbee devices over its Zigbee radio and relays messages to and from ZServer. A secondary controller can also run the ZAP process (but not ZServer), in order to act as a remote Zigbee access point (“additional ZAP”).

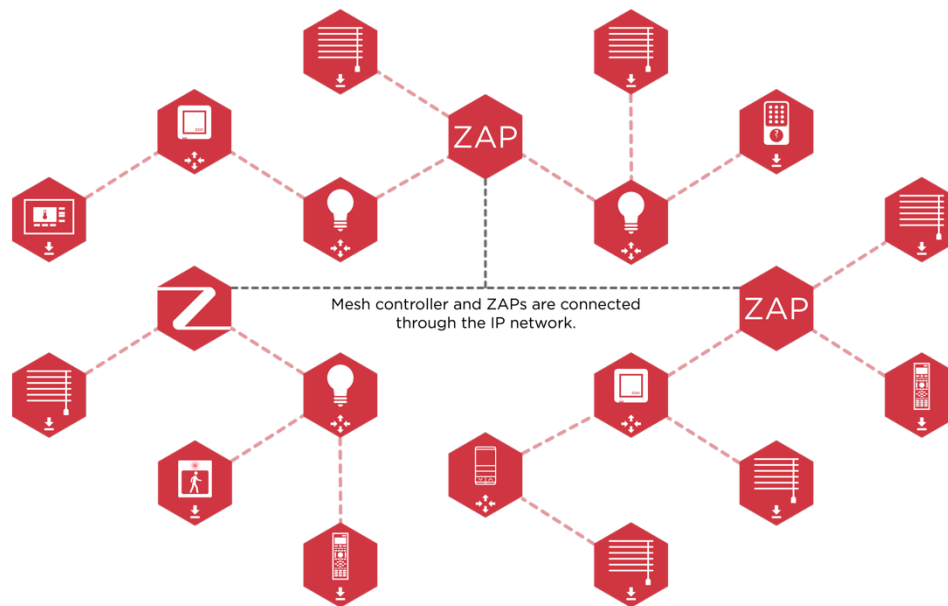
ZServer—A software process on a mesh controller that handles commands to and from the Control4 project and sends those commands to the ZAP. Only one ZServer can be configured in a single mesh, configuring a second ZServer will create a separate Zigbee mesh network.



Note: The additional ZAP controllers all communicate to the same Zserver on the primary mesh controller, so they all share the same security key as the primary mesh controller. Devices that have joined to the mesh can talk to either the primary mesh controller or the additional ZAPs.

Multiple ZAP example

One mesh controller and two ZAPs sharing the same security key



Multiple ZAP use case 1: Roaming remotes

In a design with multiple mesh controllers, each mesh network has its own security key, so a remote control would work only in the mesh where it was identified. This issue prevents the use of a remote outside its native mesh, which can be problematic in a large home with multiple meshes.

One way to deal with this problem is to assign remotes to particular areas or rooms and use them only in those areas.

Another way is to enable secondary controllers to act as additional ZAPs.

An additional ZAP has the same design requirements as a mesh controller:

- Total number of devices is less than 70 (total devices per Zigbee mesh).
- Place the ZAP central to the Zigbee devices to control.
- Avoid WiFi interference.
- Do not put the ZAP in an equipment rack.

Multiple ZAP use case 2: Large lighting scenes

Lighting scenes can experience a delay when activated if some lights in the scene are on different meshes. Lighting scenes are activated by sending out a single command ("execute lighting scene XYZ," for example), and each lighting device remembers whether it is a part of that scene. When the same command is sent to multiple mesh controllers, latency between meshes may prevent the scene from activating at exactly the same time, so one mesh will activate the scene a short time before the second mesh activates it.

In rare cases, if the project has lights across a large area joined together in lighting scenes, instead of creating multiple mesh controllers, enable additional ZAPs. This way, lighting scene commands are sent at the same time and lights should all respond in unison. This is usually not a problem, however.

Terms and definitions

EmberNet—Supplier of Zigbee® semiconductors, software, and development tools (used to refer to original Control4 Zigbee devices). The term EmberNet is used in Control4 materials to describe legacy Control4 Zigbee devices (prior to Zigbee PRO).

Refer to the Knowledgebase (kb.control4.com) for information about EmberNet devices.

end node—A Zigbee device that does not route communication from other Zigbee devices. Devices that are powered by batteries are almost always end nodes; for example, remotes, Z2C, and door locks.

hop—The transmission of data from one device to another device in a Zigbee mesh, for example, from one light switch to another or from a system remote control to a controller.

mesh topology—Network topology where each device communicates directly with any other within range, allowing network traffic to be shared with each device and with the mesh controller.

router node—A Zigbee device that relays Zigbee communication from one or more Zigbee devices to another Zigbee device, making a path back to a mesh controller (or directly communicating with a mesh controller).

sleepy (“non-polling”) node—An end node that wakes up its Zigbee radio only when it communicates to its routing node or the mesh controller.

star topology—Network topology where each wireless device must communicate to the router via a wireless access point.

topology—The path that data takes in order to travel around the network. See *mesh topology* and *star topology*.

ZAP (Zigbee access point)—A software process that runs on a Control4 controller and controls the Zigbee radio. A ZAP communicates with Zigbee devices over the Zigbee radio and relays messages to and from ZServer. See *ZServer*.

ZAP coordinator—The first ZAP created during Zigbee mesh configuration, which is responsible for setting up the security parameters of the mesh and also communicates with Zigbee devices. See *ZAP*.

Zigbee—A wireless network that uses bi-directional wireless mesh network technology to transfer messages from one device to another. A mesh network topology allows the devices to forward messages from one device to another, thereby extending the effective range of the network.

Zigbee mesh—A term for a Zigbee wireless network. A Zigbee mesh network includes a mesh controller and other Zigbee devices.

Zigbee mesh controller—A Control4 controller that acts as the Zigbee mesh’s communications gateway. Each mesh controller runs the ZServer and ZAP processes. Control4 recommends having both ZServer and ZAP running on the same controller.

Zigbee PRO—The 1.1 version of Zigbee that provides improvements in standardization by allowing more interoperability with other Control4 devices, support for home automation profiles, and improves the scalability of multiple Zigbee access points.

ZServer—A software process on a Control4 controllers that handles commands to and from the Control4 project and sends those commands to the ZAP. See [ZAP](#).

Legal notices

This document is confidential and is only made available to authorized Control4 Dealers who have agreed to terms of confidentiality under the Control4 Non-Disclosure Agreement. These terms must be maintained and pertain to information found in this document.

Information in this document, including URL and other Internet website references, is subject to change without notice and is provided for informational purposes only. The entire risk of the use or results of the use of this document remains with the user, and Control4 makes no warranties, either express or implied.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Control4.

Control4 may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Control4, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

This document is for reference purposes only, and it is provided only as advice to Dealers. Each system setup is unique and customized to a specific customer's needs. It is the Dealer's responsibility to make sure the system is compatible before making any changes and installing any updates. In addition, it is the Dealer's responsibility to get the customer's permission before accessing the customer's system and making any changes or installing any updates.

About Control4®

Control4 Corporation is a leading global provider of automation and networking systems for homes and businesses, offering personalized control of lighting, music, video, comfort, security, communications, and more into a unified smart home system that enhances the daily lives of its consumers. Control4 unlocks the potential of connected devices, making networks more robust, entertainment systems easier to use, homes more comfortable and energy efficient, and provides families more peace of mind. The Control4 platform interoperates with more than 13,000 third-party consumer electronics products, ensuring an ever-expanding ecosystem of devices will work together. Leveraging a professional channel that includes over 5,800 custom integrators, retailers, and distributors authorized to sell Control4 products, Pakedge networking solutions and Triad speakers, Control4 is delivering intelligent solutions for consumers, major consumer electronics companies, hotels, and businesses around the world.

Disclaimer

Control4 makes no representations or warranties with respect to this publication, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Control4 reserves the right to make changes to any and all parts of this publication at any time, without any obligation to notify any person or entity of such changes.

Licenses

Open Source

Certain items of independent, third-party code may be included in the Software that are subject to the GNU General Public License ("GPL") or other open source licenses ("Open Source Software"). The Open Source Software remains subject to the terms of the license that accompanies such Open Source Software. Nothing herein limits your rights under, or grants you rights that supersede, the terms and conditions of any applicable end user license for such Open Source Software. In particular, nothing herein restricts your right to copy, modify, and distribute such Open Source Software that is subject to the terms of the applicable license (available at www.control4.com/opensource).

Spread

This product may use software developed by Spread Concepts LLC for use in the Spread toolkit. For more information about Spread see <http://www.spread.org>.

DISCLAIMER—THIS SOFTWARE IS PROVIDED BY THE APPLICABLE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright

Copyright ©2019, Control4 Corporation. All rights reserved. Control4, Pakedge, Triad and their respective logos are registered trademarks or trademarks of Control4 Corporation in the United States and/or other countries. 4Store, 4Sight, Control4 My Home, Mockupancy, and BakPak are also registered trademarks or trademarks of Control4 Corporation. Other names and brands may be claimed as the property of their respective owners. All specifications subject to change without notice.

Control4 Zigbee PRO Best Practices and Design Guide

Contact Information

Control4 Corporation
11734 S. Election Road
Salt Lake City, UT 84020 USA
<http://www.control4.com>

Control4 Zigbee PRO Best Practices and Design Guide
DOC-00104-D
2019-04-18 DH