Challenges and Potential Solutions for Deploying IoT in a Multi-Dwelling Setting

A technical paper prepared for presentation at SCTE TechExpo24

Jeff A. Hales
Principal Architect
Cox Communications, Inc.
Jeff.hales@cox.com

Gregory Jungwirth
Solution Architect
Cox Communications, Inc.
gregory.jungwirth@cox.com

Ramon Gaubert
Senior Communications / Network Engineer
Cox Communications, Inc.
ramon.gaubert@cox.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

List of Tables

Title **Page Number**

1. Introduction

In the current competitive landscape, Multi-Dwelling Unit (MDU) owners and management companies are continuously searching for ways to motivate residents to sign new or resign existing leases at their properties versus signing with a competitor. Some of these owners/companies are leaning on service providers to offer advanced automation and integrated services that can simplify and enhance a resident's daily experience and streamline the management of these services for the staff. These advanced automation and integrated services enable personalized access to the property's gym, pool, and other amenities, as well as control of lighting, door locks and Heating, Ventilation and Cooling (HVAC) using Internet of Things (IoT) technologies within the resident's apartment/rental unit. However, these services require an Always-On Network (AON) connection (to the Internet) to ensure their associated systems are kept online (24-7) for effective real-time management and control; particular for those systems within an apartment/rental unit, regardless of whether the unit is occupancy or not. AON implementations can vary from property to property, depending on a target property's construction, layout, age, and implementation budget, which can make it a challenge to deploy and manage to ensure reliability.

This paper will discuss several of the associated challenges and solutions in deploying and managing an AON connection for IoT services in MDU properties, covering deployment models as well as some pros and cons of each. Cost details will not be covered within this paper.

2. Background

To meet the evolving needs of its MDU customers, service providers have been researching and investing in new product offerings and technologies for as long as they have been in business.

Some of the technologies researched and/or utilized include: Zigbee, Z-Wave, LoRaWAN, Bluetooth, Bluetooth Low Energy (BLE), Near Field Communications (NFC), Thread, Matter, PowerG, and updated variations of Wi-Fi, Ethernet, and cellular. The knowledge acquired associated with these technologies and/or forming strategic partnerships with experts in the field has made it possible for some service providers to expand their residential and commercial portfolios with IoT-based solutions, such as home/business security and automation. These solutions enable a broad set of monitoring and control capabilities (i.e., motion sensors, door/window sensors, leak sensors, lighting control, HVAC control, etc.) benefiting both resident and business owner. And when combined with many aspects of rental property life, service operators can provide a compelling, unified set of smart technology systems to help MDU communities set themselves apart from their competition.

In doing so, there is an expectation that many of these smart technology systems are always online and available for the residents, MDU staff, and associated back-office systems. The benefits offered by these systems would be diminished if they were not available to receive a critical firmware update, provide notice of a water leak in a unit to minimize property damage, allow a resident to unlock a door remotely or to remove an access code when needed. Due to this expectation, having a reliable AON connection for these systems is vital in maintaining the desired level of operational experience.

Deploying an AON in an MDU setting can be a challenge depending on the layout and construction type of a target property, the IoT system selected, the amenities to be integrated, and the Internet transport solutions available for use by the services provider. The IoT customer's experience is highly dependent on network connectivity used to support the selected IoT system; with a recent Parks research paper noting that 51% of respondents reported they experienced loss of wireless connectivity (Parks Associates, 2021).

However, with MDU properties comprising approximately 30% of homes passed in America (Parks Associates, 2021) and higher for some other countries, service providers are highly motivated to develop creative methods to deploy AON connections in support of new IoT-based solutions that can drive growth and capture market share for themselves and their MDU customers.

3. Enabling Always-On Connectivity in MDUs

A lot of work is required to deliver a reliable and effective MDU IoT solution that offers the advanced automation and integrations the multi-family industry is demanding; with a key part of the effort being the ability to deploy and manage AON connectivity for the varied systems within an MDU setting.

In scoping the effort and the opportunity, it is important to understand that MDUs include apartments, condominiums, assisted living facilities, and dormitories, which can consist of a single or multi-floor environment where multiple housing units are contained in one or more buildings that are grouped into a complex or campus. Since MDUs can vary in construction type, layout, and the complement of systems/services supported within, these and several other factors should be taken into consideration when planning AON deployments.

Some factors that should be included when defining/selecting an appropriate AON deployment model follows:

Table 1 - Key AON Enablement Factors

Key AON Enablement Factors
Property Installation Classification
Property Construction Type
Property Layout
IoT Platform Requirements
Property Amenities

Completing a site survey for each property is generally the best way to collect all the pertinent information that will help with this planning. During which time, prospective MDU property is classified as either a “Greenfield” or “Brownfield” installation project, as it can influence the deployment model (covering the specific IoT implementation and associated backhaul) used.

3.1. Property Installation Classifications

3.1.1. Greenfield

The Greenfield installation classification is traditionally given to a property that will be “built from the ground up”, “brand new” or “new build” construction project. A Greenfield property is usually in pre-construction or still in the planning stage gives the AON service provider the opportunity to make accommodations for the required infrastructure needed for the IoT solution. These deployment types are generally less constrained (except for budget) and can offer greater flexibility to provide cost savings by “doing things right the first time”.   From time-to-time challenges can arise when a service provider is engaged late in a property’s planning stage, but those situations are usually handled by successful navigation of the change management process.   With proper pre-construction planning for AON deployments Greenfield installations tend to have very few challenges, therefore no additional details will be provided for properties this classification.

3.1.2. *Brownfield*

The Brownfield installation classification is traditionally given to a property that will be a "built on existing" construction project for adding the IoT solution (and potentially network elements). This type of property has already completed its construction and can be more constrained (offering less flexibility) regarding IoT and AON deployment as they (generally) need to leverage existing physical infrastructure or may require additional time and budget if new infrastructure is needed to support the enablement of the AON depending on the property's construction type and layout.

3.2. Property Construction Types

The following table provides the common property construction types, for which MDUs typically use Type I, II, III and V (New England Institute of Technology, 2021).

Table 2 - Property Construction Types

Construction Type	**Salient Features**
Fire Resistive (Type I)	• Fire Resistive construction refers to building materials and techniques used to minimize the spread of fire and maintain the structural integrity of a building during a fire. • These constructions are designed to resist fire for a specified period; usually one to four hours, giving occupants enough time to evacuate and firefighters time to extinguish the fire. • Fire Resistive construction often uses fire-resistant concrete, brick, and steel materials.
Non-Combustible (Type II)	• Non-Combustible construction refers to building materials and techniques that do not ignite, burn, or contribute fuel to a fire. • These constructions reduce fire risk and limit its spread within a building. • Non-Combustible construction typically involves using materials such as steel, concrete, and masonry, which have a high resistance to fire and do not release harmful fumes or gases when exposed to fire.
Ordinary (Type III)	• Ordinary construction refers to building materials and techniques commonly used in buildings that are not classified as fire-resistive or non-combustible. • These constructions are designed to be functional and economical, but they may not offer the same level of fire resistance as more advanced building techniques. • Ordinary construction may use wood framing, plaster, and brick veneer. • Buildings constructed with ordinary construction methods may require additional fire safety measures, such as sprinkler systems or fire-resistant coatings.
Heavy Timber (Type IV)	• Heavy Timber construction refers to building materials and techniques that use large dimensional timber as the main structural element. • This type of construction is known for its strength, durability, and resistance to fire. • Heavy Timber construction typically uses large wooden beams, columns, and decking to create a solid and sturdy structure. The thickness of the timber provides natural fire resistance, as it chars on the outside and slows the spread of flames. • Heavy Timber construction is commonly used in churches, schools, and historic structures.
Wood Frame (Type V)	• Wood Frame Construction refers to building materials and techniques that use wood as the main structural element. • This type of construction is popular in residential and light commercial buildings due to its cost-effectiveness and ease of construction. • Wood Frame Construction typically involves using dimensional lumber, engineered wood products, or wood panels to create the framing of the building.

	• While wood is a combustible material, Wood Frame construction can be made more fire-resistant through fire-retardant treatments, sprinkler systems, and other fire safety measures.

3.3. Property Layouts and Associated Challenges

3.3.1. High-Rise MDU

3.3.1.1. Overview

High-Rise MDUs generally have more than 10 Floors and contain 128+ housing units that use an internal residential entry. Installations in these properties can be highly complex, while minimally challenging. This is due to the fact that they have planned cabling access to the various stories and sections of the buildings generally making deployment the least challenging of the layouts, as these properties typically contain a single MDF (Main Distribution Frame) room with (floor to floor) cable trunking to IDF (Intermediate Distribution Frame) rooms where equipment can be housed, which are generally environmentally controlled with centralized temperature monitoring, providing the optimal conditions for traditional networking equipment. High-Rise properties tend to have some of the most stringent construction parameters and require a fire resistive construction type (Type I).

3.3.1.2. Typical Challenges

Some of the typical challenges for a High-Rise MDU are as follows:

- In older buildings, the MDF to IDF planning model might not exist.
- Cabling pathways could be filled with existing wire.
- Insufficient environmental controls
- Increased sources of interference
- Structural steel and metallic studs can make signal TX/RX difficult with some IoT protocols.

3.3.2. Mid-Rise

3.3.2.1. Overview

Mid Rise MDUs generally have up to 10 floors and contain 12-128 housing units that use an internal residential entry. Installation in these properties can range from medium to high complexity, while being moderately challenging. Like High-Rise MDUs, Mid-Rise MDUs generally have an MDF to IDF planning model with environmental controls. However, older buildings tend to be “walk-ups” (buildings with no elevator thus no shaft to use for cable routing) for which a planning model might environment controls may not exist. Mid-Rise properties require a fire resistive construction type (Type I).

3.3.2.2. Typical Challenges

Some of the typical challenges for a Mid-Rise MDU are as follows:

- In older buildings, the MDF to IDF planning model might not exist or the building may only have IDF closets.
- In some cases, cable routing may need to be done externally which can require weatherproof enclosures, conduit, and fittings.
- Cabling pathways might not exist.
- Cabling pathways could be filled with existing wire.

- Insufficient/Non-existent environmental controls in dedicated equipment spaces in older buildings (generally telecom closets)
- Increased sources of interference
- Structural steel and metallic studs can make signal TX/RX difficult with some IOT protocols.

3.3.3. Low-Rise / Garden-Style MDUs

3.3.3.1. Overview

Low-Rise or Garden-Style MDUs typically have no more than 4 floors with less than 12 housing units that leverage an external residential entry. Installation at these properties tends to be of medium to low complexity, but the challenges can range from moderate to high. Newer buildings are planned for cabling access, but older buildings generally are not, making it difficult to deploy AON connectivity. In cases where cabling access is not provided, creative installation measures need to be utilized that are cost effective and retain the aesthetic integrity of the property and units. Low-Rise / Garden-Style properties may not have MDF's or IDF's, and they may not have an environmentally controlled space for housing equipment unless they are relatively new. Typically, network infrastructure equipment is mounted on external walls in secure enclosures, or in attic/crawl spaces. These properties tend to use Ordinary (Type III) or Wood framed (Type V) construction types.

3.3.3.2. Typical Challenges

Some of the typical challenges for a Low-Rise / Garden-Style MDU are as follows:

- Non-existent MDF/IDF
- Cabling pathways might not exist.
- Cabling pathways could be filled with existing wire.
- In most cases, cable routing needs to be done externally which will require weatherproof enclosures, conduit, and fittings.
- Increased sources of interference

3.4. IOT System Requirements

Service providers have numerous IoT system options to choose from when determining what they will use to satisfy the MDU industry's needs. While most service providers will choose to partner with a 3rd party, some may decide to develop their own system - giving them full over the MDU-IoT implementation. There is a long list of pros and cons associated with the choice, but regardless of the path, the IoT systems utilized will be grounded with a feature set driving by the end-user's needs. Coupled with other business requirements, this feature set will also drive decisions associated with the operation of the MDU-IoT implementation - including the AON deployment model. These operational and installation considerations can vary from system to system, depending on the IoT technologies used and capabilities implemented and can be documented as constraints.

3.4.1. Constraints

In considering the utilized IoT system, several constraints may need to be imposed to help minimize potential operational and customer experience impacts for an MDU-IoT implementation. Some examples of commonly imposed constraints are as follows:

- The IoT system should operate over the top (OTT) of existing services, if transport is shared.

- IoT Hubs/Gateways must utilize a wired broadband connection as its primary transport path, to minimize potential impacts due to wireless operational concerns (i.e. interference, wireless management/changes, etc.).
- IoT Hubs/Gateways may utilize a wireless broadband connection as its secondary transport path.
    - Cellular is available for some IoT solutions
- IoT technology diversity should be supported
    - Primary: Zigbee
    - Secondary: Z-Wave when required by Property
- Firewall functionality may be required for the utilized IoT system
    - The requirement to use a firewall may be driven by the IoT system's vendor or a service provider's Information Security organization due to limitations of the associated IoT Hub or other IoT infrastructure.
- IoT Hub/Gateway traffic must be secure (traffic encrypted), as the transport may be shared
- AON and IoT elements should both support IPv4 and IPv6
- Operational environment for deployed equipment MUST be considered
    - IDF/MDF temperatures may not be controlled
    - Smart enclosures may not be ventilated
    - AON transport and IoT gear are generally not temperature hardened

While these considerations/constraints may not apply to every deployment, they can be used as a guideline or initial reference when reviewing AON deployment options.

3.5. Property Amenities

While the focus of this paper is on enabling IoT functionality within an MDUs rental units, the MDU owners/companies and their residents desire a more unified experience for all systems they may interact with daily. These systems often include access control for the gym, pool, and the entry/exit gate, as well as community Wi-Fi, each all have their own set of connectivity and integration requirements. While practical experiences with these systems may currently be limited for some service providers, the deployment models present below can be used to address these systems connectivity needs.

4. Deployment Models

Taking into consideration the business goals, customer needs, timelines, and the AON Deployment Factors (presented above), a number of deployed models were constructed and vetted by Cox Communications, with some approved for deployment. While many of these deployment models are rooted in standard Internet delivery methods used by various service providers, the construction and validation of these deployment models was a necessary step in the MDU-IoT journey, as "every property is different" (due to its property classification, construction type, and layout) and can have their own unique and challenging characteristics. This journey and the knowledge resulting from these unique property experiences have resulted in refinement of these models, and the creation of newer deployment models that best suit the business needs.

Note: Some of these deployment models are centric to DOCSIS® technologies and therefore may not be application for all service providers. In addition, any provisioned service/speed tiers specified within these deployment models were selected based on the data needs of the selected IoT platform and was readily available; however, each service provider will need to determine what service/speed tiers work best for their selected solution elements.

4.1. DOCSIS Dual-Line Drop

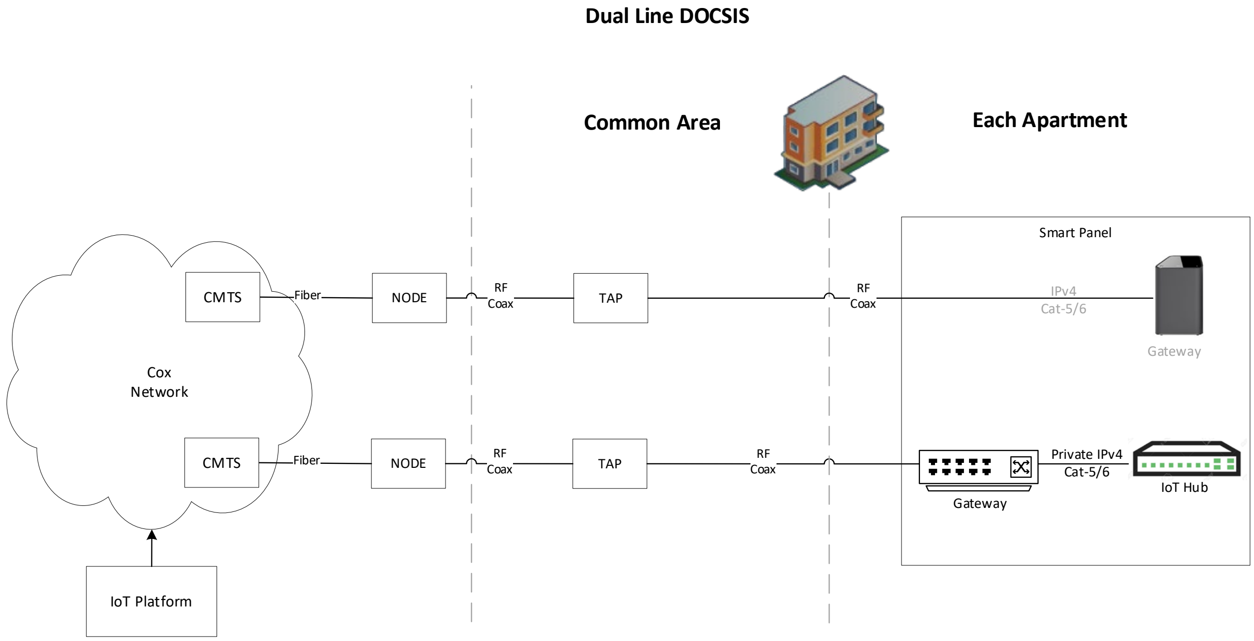

Figure 1 - DOCSIS Dual-Line Drop

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: DOCSIS + Gateway
- IoT Devices: IoT Hub
- Provisioned Internet Speed: 10 Mbps Downstream / 2 Mbps Upstream
- IP Setup: IPv4/IPv6 for Gateway, Private IPv4/IPv6 for IoT Hub
- Cost: $$$

Notes: Dual line drop was the earliest developed deployment model. One cable drop for customer Internet and one cable drop for IoT service. The dual line drop was required due to the initial provisioning constraint that AON service was not available on a normally provisioned customer Internet service. Without an AON connection Internet for the IoT service, the IoT service would be disconnected when the resident moved out of the unit.

PROs: Simple deployment model using existing Internet Service tiers.
Dedicated to AON

CONs: Expensive to run a second cable to every unit and have two Gateways in each unit.

4.2. Fiber Dual-Line Drop

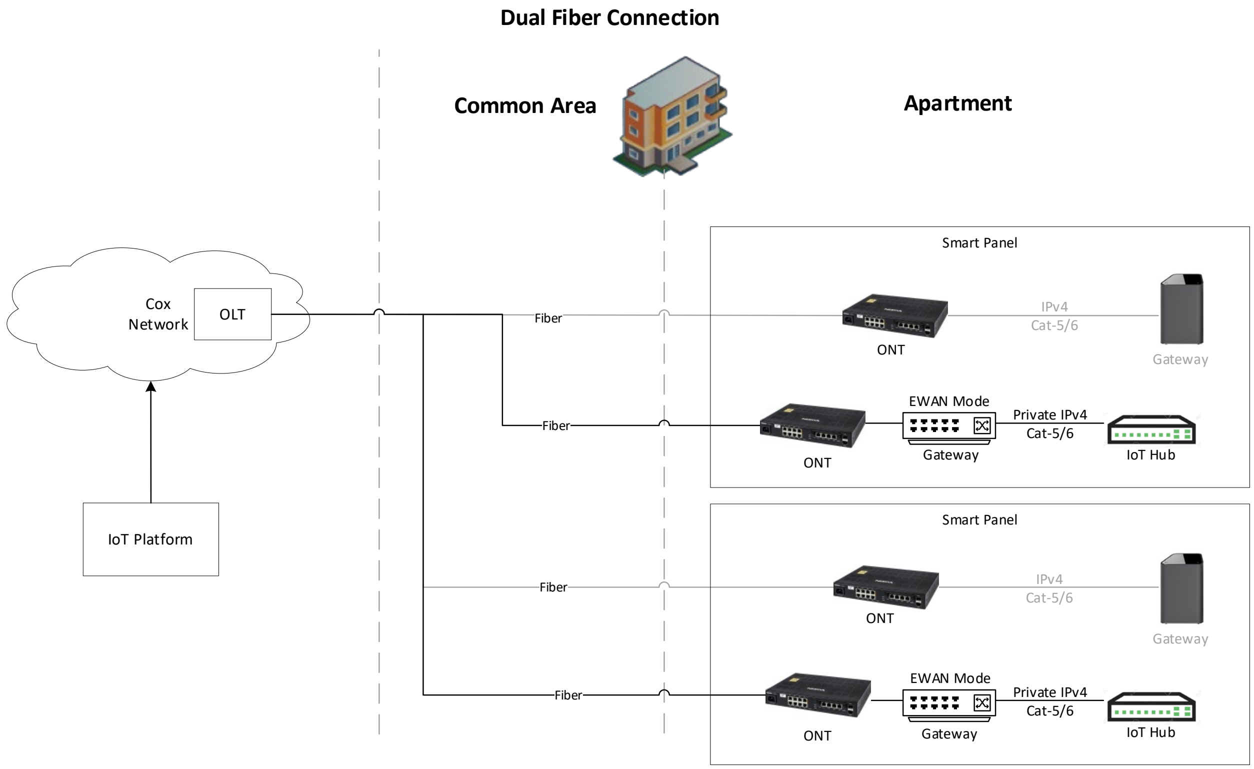

Figure 2 - Fiber Dual-Line Drop

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: Fiber (IP/RFOG/PON) + ONT + EWAN Gateway in each unit
- IOT Devices: IoT Hub
- Provisioned Internet Speed: 5 Mbps Downstream / 5 Mbps Upstream
- IP Setup: Routable IPv4/IPv6 for ONT, Routable IPv4/IPv6 for Gateway, Private IPv4/IPv6 for IoT Hub
- Cost: $$$

Notes: Dual line drop was the earliest deployment model. One cable drop for customer Internet and one cable drop for IoT service. The dual line drop was required due to the initial provisioning constraint that AON Internet service was not available on a normally provisioned customer Internet service. Without AON Internet for the IoT service, the IoT service would be disconnected when the resident moved out of the unit.

PROs: Simple deployment model using existing Internet Service tiers.
Dedicated AON connection

CONs: Expensive to run a second cable to every unit and have two Gateways in each unit.

4.3. Fiber with Switched Ethernet

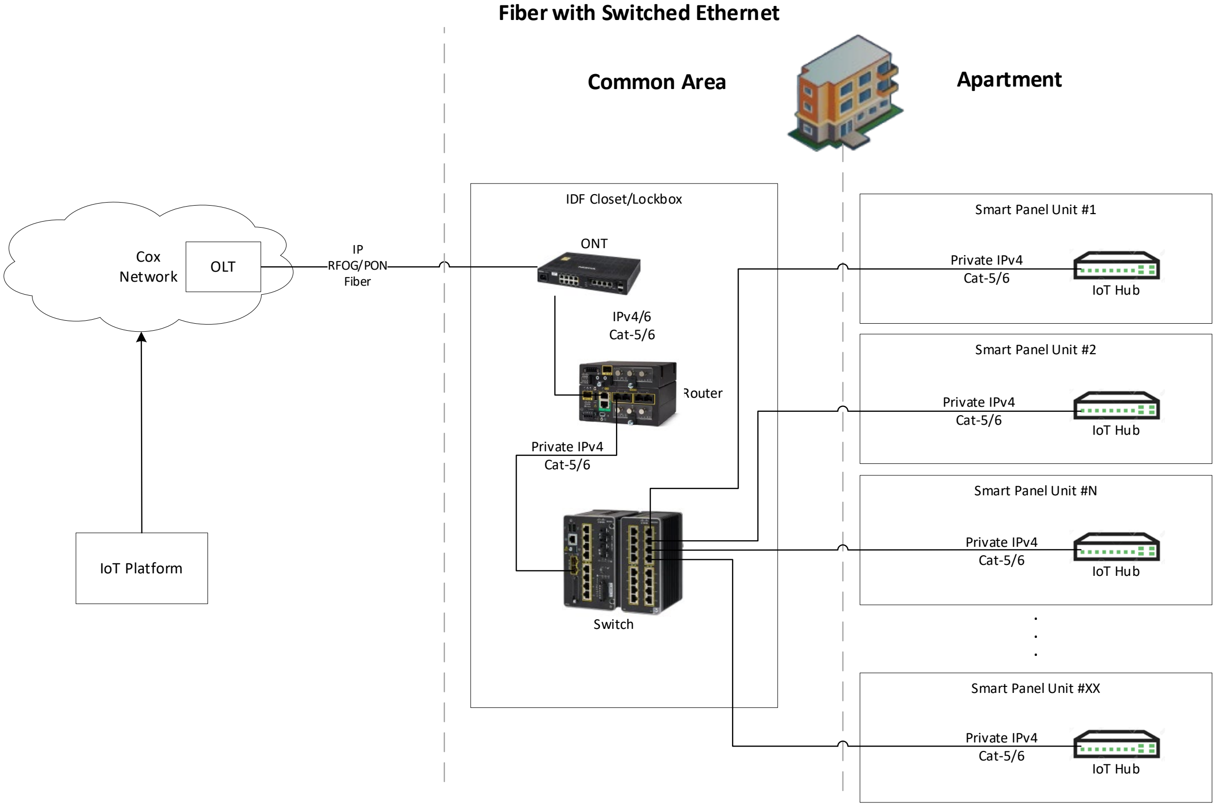

Figure 3 - Fiber with Switched Ethernet

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: Fiber (IP/RFOG/PON) + Temperature Hardened ONT, Router, and Switch(es) – multiple switches are supported by the router to service additional units (up to 96 units with selected devices)
- IOT Devices: IoT Hub
- Provisioned Internet Speed: 100 Mbps Downstream / 100 Mbps Upstream
- IP Setup: Routable IPv4/IPv6 for ONT, Static Routable IPv4/IPv6 for Router, Static Routable IPv4/IPv6 for Switches, Private IPv4/IPv6 for IoT Hub
- Switches (1-4) have Port Mapped access through the router for SSH and SNMP
- Cost: $$$$

Notes: This deployment model is used mainly in brownfield deployments that have many units in one building with existing ethernet cabling to each unit terminating in a common location.

PROs: Only requires one Internet line per router deployment.
Can deploy multiple Router/Switch configurations to support additional units.
Simple deployment model using existing Internet Service tiers.
Simple Internet service monitoring solutions are normally available for the commercial router.

CONs: Expensive to deploy temperature hardened devices that are required for many deployments.
This Deployment Model dedicated to only provide for IoT service (no customer Internet service).

4.4. DOCSIS Single Line Drop

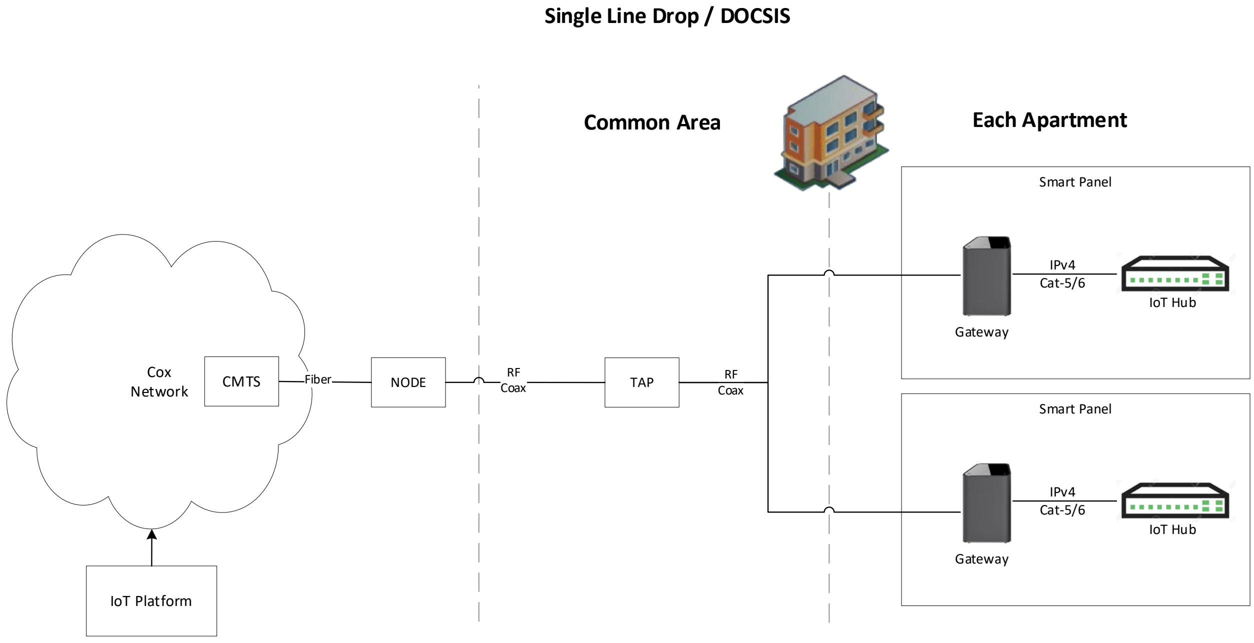

Figure 4 - DOCSIS Single Line Drop

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: DOCSIS + Gateway in each unit
- IoT Devices: IoT Hub
- Internet Speed - IoT Low Speed Tier
  - Note: Internet will be provisioned with the Internet tier purchased by the Resident. The IoT Low Speed tier is provisioned when there is no Resident in the unit, or the resident does not take Internet service.
  - Provisioned IoT Internet Speed: 3 Mbps Downstream / 3 Mbps Upstream
  - Wi-Fi is disabled when there is no resident in the unit
- IP Setup: Routable IPv4/IPv6 for Gateway, Private IPv4/IPv6 for IoT Hub
- Cost: $ (Assumes residential Internet service gear is planned or in place)

  Notes: This is the preferred IoT deployment model. Development was needed for the Provisioning system to be able to distinguish between periods of live resident Internet service and periods with no resident or when the resident does not take Internet service so that the IoT Low Speed tier can be provisioned to the gateway. Equipment to maintained on house account. Wi-Fi disabled when no resident in the unit.

PROs: Only requires one Internet line per unit.
IoT Internet service rides Over-the-Top (OTT) of the customer Internet service.
The Gateway is pre-deployed for Internet service and is not paid for by IoT, making this a low cost IoT solution.

CONs: The Property Manager must select a pre-deployed Internet offering for this deployment model.

IoT traffic would count against usage-based billing, (if enabled) however, traffic volume would be low

4.5. Fiber Single Line Drop

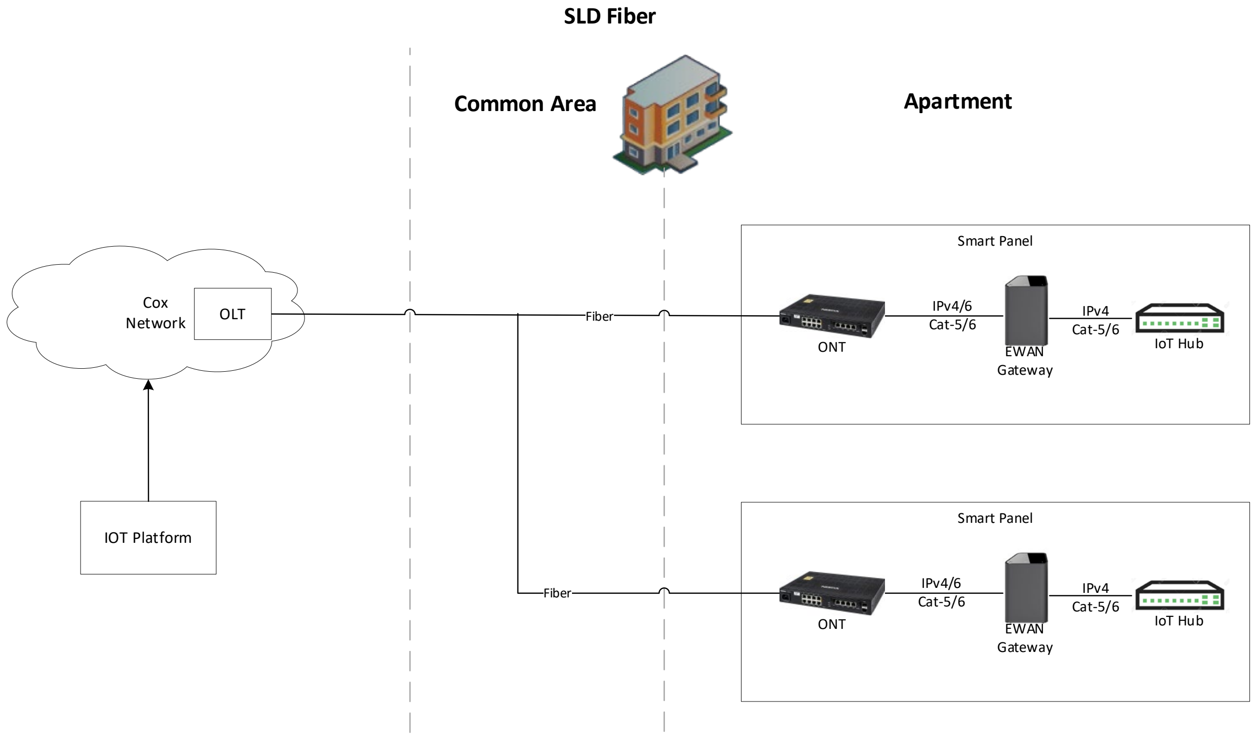

Figure 5 - Fiber Single Line Drop

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: Fiber (IP/RFOG/PON) + ONT + EWAN Gateway in each unit
- IoT Devices: IoT Hub
- Internet Speed - IoT Low Speed Tier
    - Note: Internet will be provisioned with the Internet tier purchased by the Resident. The IoT Low Speed tier is provisioned when there is no Resident in the unit, or the resident does not take Internet service.
  - Provisioned IoT Internet Speed: 3 Mbps Downstream / 3 Mbps Upstream
- IP Setup: Routable IPv4/IPv6 for ONT, Routable IPv4/IPv6 for Gateway, Private IPv4/IPv6 for IoT Hub
- Cost: $ (Assumes residential Internet service gear is planned or in place)

Notes: This is a preferred IoT deployment model. Development was needed for the Provisioning system to be able to distinguish between periods of live resident Internet service and periods with no resident or when the resident does not take Internet service so that the IoT Low Speed tier can be provisioned to the gateway. Equipment to maintained on house account. Wi-Fi disabled when no resident in the unit.

PROs: Only requires one Internet line per unit.
IoT Internet service rides Over-the-Top (OTT) of the customer Internet service.
The Gateway is pre-deployed for Internet service and is not paid for by IoT, making this a low cost IoT solution.

CONs: The Property Manager must select a pre-deployed Internet offering for this deployment model.

IoT traffic would count against usage-based billing, (if enabled) however, traffic volume would be low

4.6. DOCSIS Managed Wi-Fi

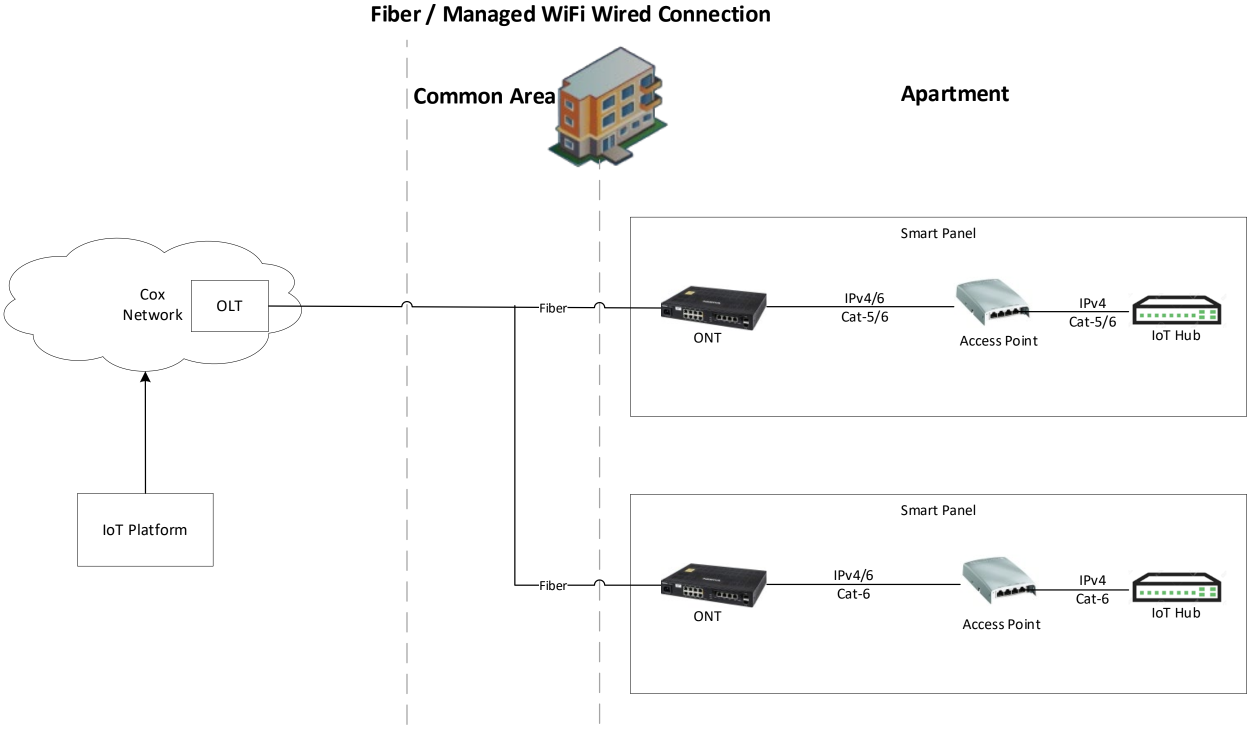

Figure 6 - DOCSIS Managed Wi-Fi

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: DOCSIS + Cable Modem + Access Point
- IoT Devices: IoT Hub
- Provisioned Internet Speed: Speed set by Managed Wi-Fi contract
- IP Setup: Routable IPv4/IPv6 for CM, Routable IPv4/IPv6 for AP, Private IPv4/IPv6 for IoT Hub
- Assumption: Managed Wi-Fi would be completely installed prior to the IoT Hub
- Assumption: Firewall functionality supported in Managed Wi-Fi platform
- Cost: $

Notes: This deployment model is approved, but not yet deployed.
PROs: Only requires one Internet line per unit.
IoT Internet service rides Over-the-Top (OTT) of the customer Internet service.
The AP is pre-deployed for Managed Wi-Fi service and is not paid for by IoT, making this a low cost IoT solution.
CONs: The Property Manager must select the Managed Wi-Fi offering for this deployment model.
If usage-based billing, IoT traffic would count against the usage

4.7. Fiber Managed Wi-Fi

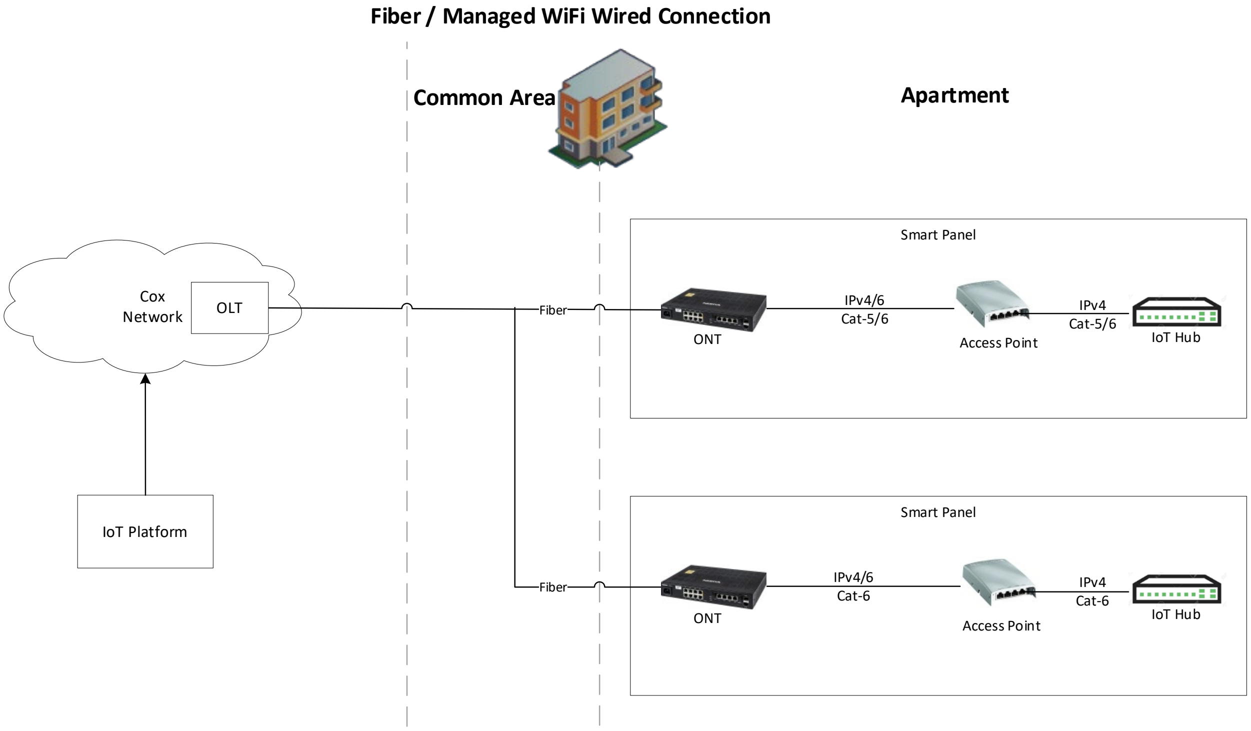

Figure 7 - Fiber Managed Wi-Fi

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: Fiber + ONT + Access Point
- IoT Devices: IoT Hub
- Provisioned Internet Speed: Speed set by Managed Wi-Fi contract
- IP Setup: Routable IPv4/IPv6 for CM, Routable IPv4/IPv6 for AP, Private IPv4/IPv6 for IoT Hub
- Assumption: Managed Wi-Fi would be completely installed prior to the IoT Hub
- Assumption: Firewall functionality supported in Managed Wi-Fi platform
- Cost: $

Notes: This deployment model is approved, but not yet deployed.
PROs: Only requires one Internet line per unit.
IoT Internet service rides Over-the-Top (OTT) of the customer Internet service. The AP is pre-deployed for Managed Wi-Fi service and is not paid for by IoT, making this a low cost IoT solution.
CONs: The Property Manager must select the Managed Wi-Fi offering for this deployment model.
If usage-based billing, IoT traffic would count against the usage

4.8. Fiber Managed Wi-Fi with Wi-Fi IoT Hub

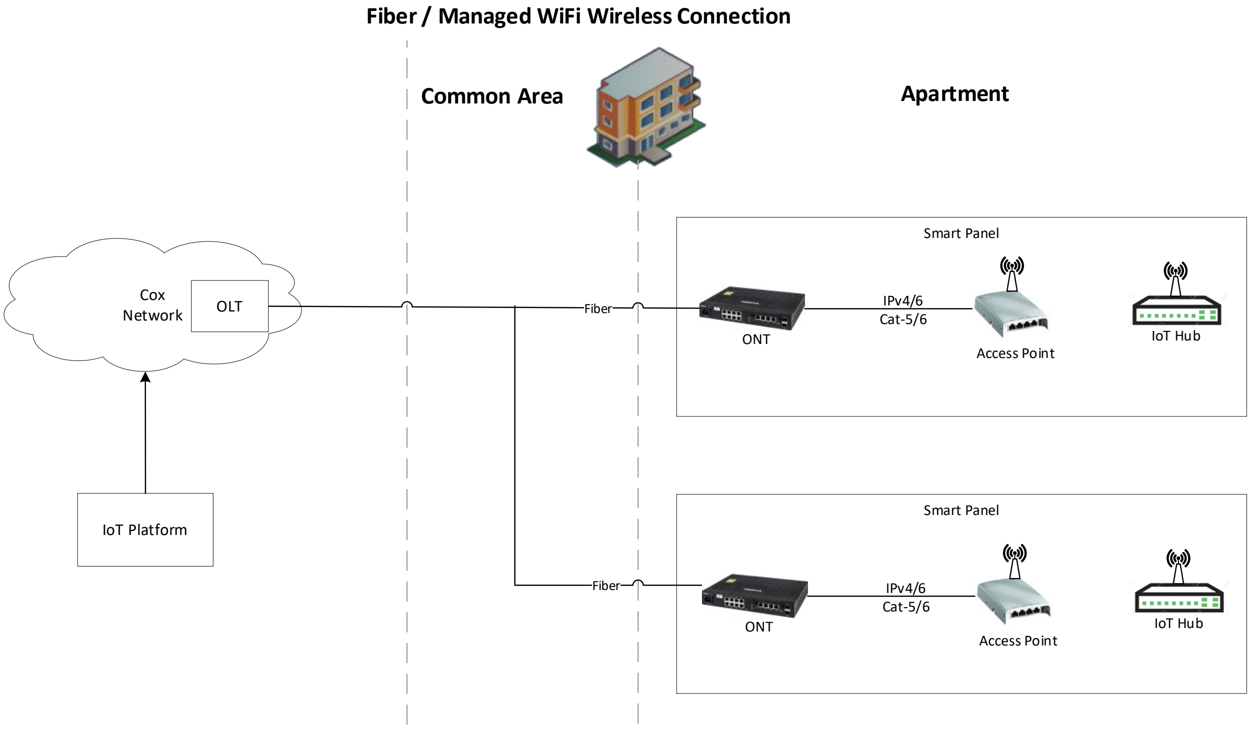

Figure 8 - Fiber Managed Wi-Fi with Wi-Fi to IoT Hub

Deployment Model Considerations:

- Deployment Status: **Under Investigation**
- Transport: Fiber + ONT + Access Point
- IoT Devices: Wireless IoT Hub
- Provisioned Internet Speed: Speed set by Managed Wi-Fi contract
- IP Setup: Routable IPv4/IPv6 for ONT, Routable IPv4/IPv6 for AP, Private IPv4/IPv6 for IoT Hub
- Assumption: Managed Wi-Fi would be completely installed prior to the IoT Hub
- Assumption: Firewall functionality supported in Managed Wi-Fi platform
- Cost: $

Notes: This deployment model is NOT approved for deployment. Current IoT Hub do not support Wi-Fi connectivity, therefore cannot be tested.
PROs: Only requires one Internet line per unit.
IoT Internet service rides Over-the-Top (OTT) of the customer Internet service.
The AP is pre-deployed for Managed Wi-Fi service and is not paid for by IoT, making this a low cost IoT solution.
CONs: The Property Manager must select the Managed Wi-Fi offering for this deployment model.
The IoT Hub must be Wi-Fi enabled.

4.9. DOCSIS Thread-Mesh

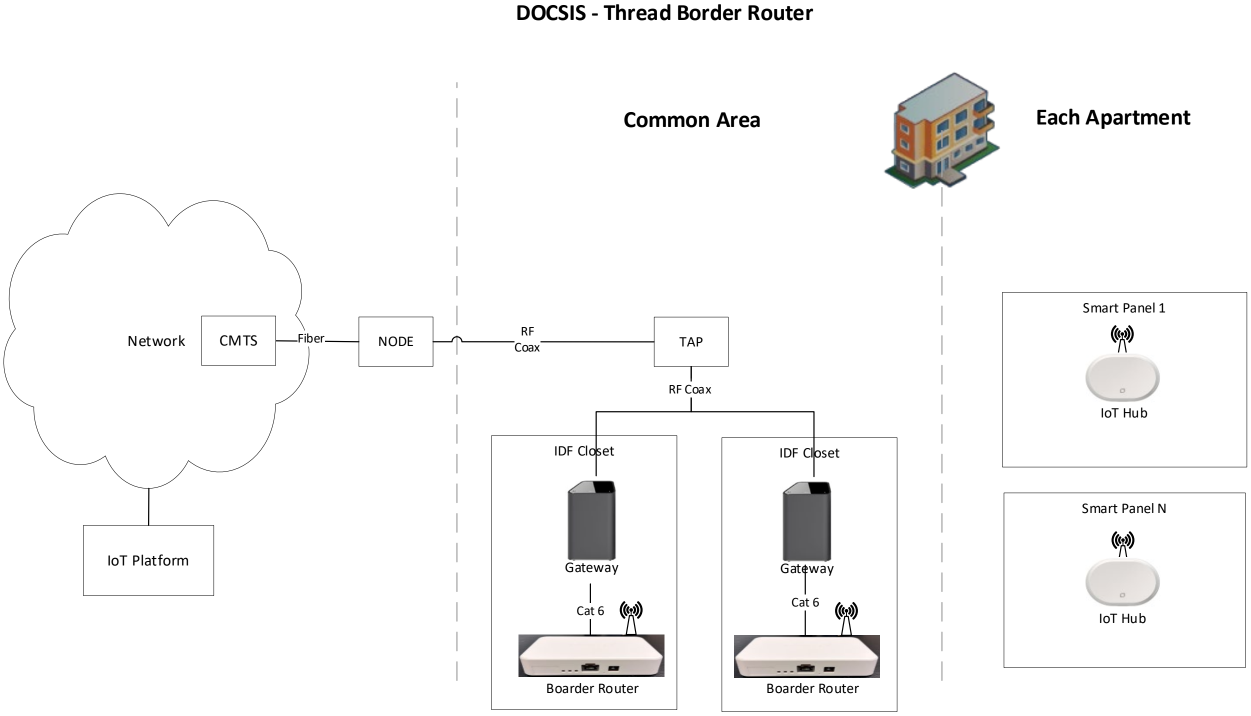

Figure 9 - DOCSIS Thread-Mesh

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: DOCSIS + Gateway (in an IDF)
- IoT Devices: Thread Border Router (in an IDF), Wireless Thread IoT Hub (in each unit)
- Provisioned Border Router Internet Speed
    - Sub/Mid Split: 100 Mbps Downstream / 10 Mbps Upstream
    - High Split: 100 Mbps Downstream / 100 Mbps Upstream
- IP Setup: Static Routable IPv4/IPv6 for Gateway, Private IPv4/IPv6 for Border Router
- Cost: $

Notes: This deployment model utilizes Thread Border Routers to connect to the IoT Hub. The Thread Border Routers and Thread IoT Hubs are setup in a mesh configuration. The Border Routers are recommended to be redundant, but automated failover is still in development.

PROs: Only requires one Internet line per Border Router.
Low cost as each Border Router can service multiple IoT Hubs).

CONs: The Thread Border Router only provides connectivity for the IoT Hubs (no customer Internet service).
Limited number of IoT Hubs per Border Router.
Limited range of the Thread Border Router to IoT Hub connection.
MDU construction type could limit Mesh Thread connectivity

4.10. Fiber Thread-Mesh

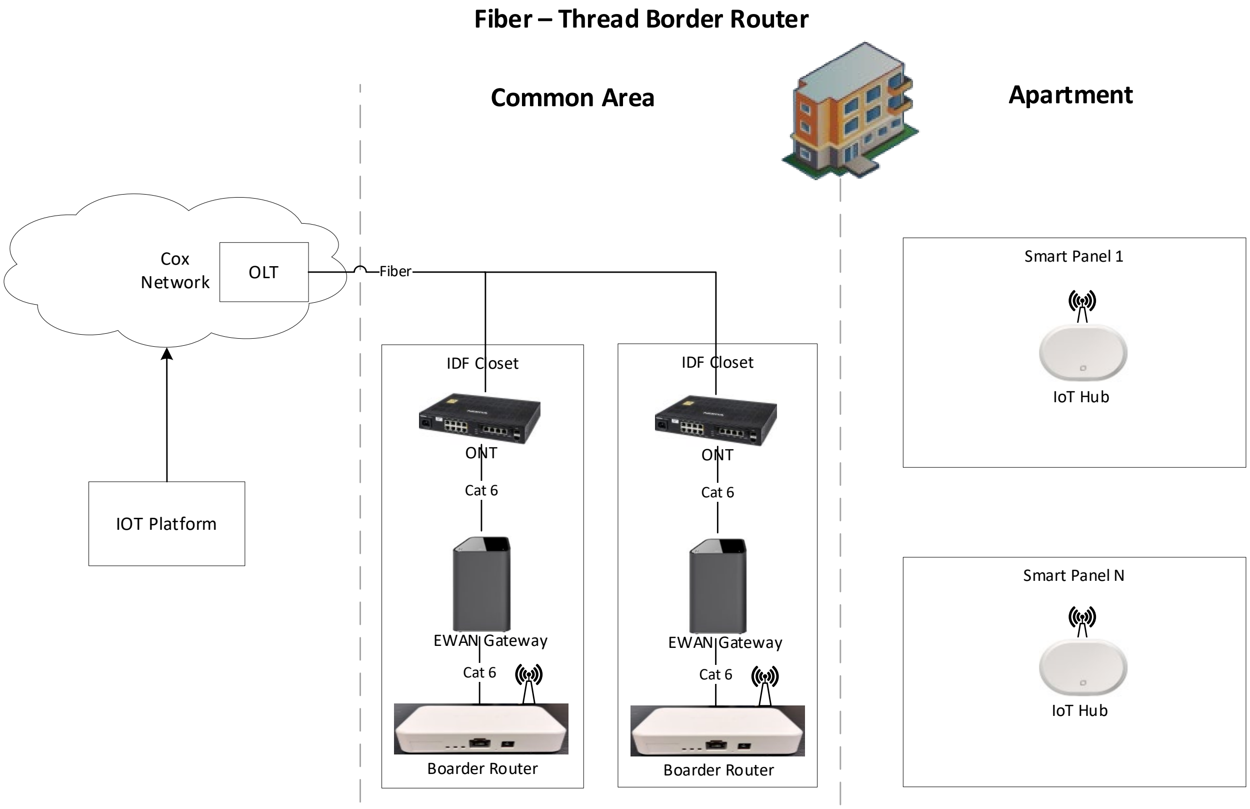

Figure 10 - Fiber Thread-Mesh

Deployment Model Considerations:

- Deployment Status: Approved for Deployment
- Transport: Fiber (IP/RFOG/PON) + ONT + EWAN Gateway (in an IDF)
- IoT Devices: Thread Border Router (in an IDF), Wireless Thread IoT Hub (in each unit)
- Provisioned Border Router Internet Speed: 100 Mbps Downstream / 100 Mbps Upstream
- IP Setup: IPv4 for ONT, IPv4 for EWAN Gateway, Private IPv4 for Thread Border Router
- Cost: $ (IoT only)

Notes: This deployment model utilizes Thread Border Routers to connect to the IoT Hub. The Border Routers are recommended to be redundant, but automated failover is still in development.

PROs: Only requires one Internet line per Border Router.
Low cost as each Border Router can service multiple IoT Hubs.

CONs: The Thread Border Router only provides connectivity for the IoT Hubs (no customer Internet service).
Limited number of IoT Hubs per Border Router.
Limited range of the Thread Border Router to IoT Hub connection.
MDU construction type could limit Mesh Thread connectivity

5. Summary

Many factors can influence the type of deployment used for an MDU-IoT implementation. Some of these factors include whether a property is classified as a Brownfield vs. Greenfield deployment, building construction type, number of units in each building, cabling options, and the characteristics of the IoT solution being deployed. There are many possible deployment models that can be used enable an AON connectivity, so it is important to standardize on a few models to reduce the complexity of supporting the MDU-IoT deployments.

This paper dove into some of the challenges and solutions of deploying an Always-On Network for IoT services in Multi-Dwelling Unit properties. MDU owners aim to improve resident experiences and increase operational efficiency through the use of IoT technologies that allow automated access to amenities (e.g. access control for things like gates and pools) and remote property management. However, achieving (and maintaining) reliable AON connectivity is complex and can vary depending on the technology utilized (think Z-Wave, ZigBee, etc.), property classification (e.g., high-rise, mid-rise, low-rise/Greenfield/Brownfield), and technical/product constraints related to the secure deployment of these systems.

Key points discussed include:

Enabling Always-On Connectivity: Factors influencing AON deployment include property classification (Greenfield vs. Brownfield), building layout (high-rise, mid-rise, low-rise), and IoT platform requirements. Each classification (Greenfield for new builds, and Brownfield for existing structures) presents unique challenges and opportunities.

Property Installation Classifications: Greenfield projects allow easier integration of IoT infrastructure during initial construction, while Brownfield projects involve retrofitting existing structures, which can complicate network deployment and management.

Property Construction Types and Layouts: Different construction types (Type I to Type V) affect AON deployment due to their varying fire resistance and structural characteristics. High-rise MDUs face challenges such as signal interference and cabling complexities, whereas low-rise buildings may lack dedicated equipment spaces and require innovative installation solutions.

IoT Platform Requirements: AON solutions should support a diverse IoT technologies (e.g., Zigbee, Z-Wave) and ensure secure by encrypted data transmission. Flexible deployment methods need to be leveraged to adhere to the various requirements and constraints defined for the solution.

In summary, the paper highlights the importance of customized AON solutions in MDUs to meet operational expectations and differentiate properties in a competitive market. By addressing deployment challenges and utilizing appropriate technologies, MDU owners can enhance resident satisfaction and operational efficiency through reliable IoT services.

6. Conclusion

The most important consideration for MDU-IoT deployments is maintaining an Always-On Internet connection to the IoT equipment, whether there is a resident in the unit or not. This is required to have 24-7 visibility to the associated IoT devices and to ensure the expected level of availability for resident and property staff is met.

And while several deployment models can be used, the Single-Line Drop deployment models are the most economical in provided IoT connectivity in an MDU unit, by operating Over-the-Top of the house equipment utilized to provide Internet services to the unit's resident.

Abbreviations

AON	Always On Network
AP	Access Point
BLE	Bluetooth Low Energy
CMTS	Cable Modem Termination System
DOCSIS	Data Over Cable Service Interface Specification
EWAN	Ethernet Wide Area Network
IoT	Internet of Things
IDF	Intermediate Distribution Frame
MDF	Main Distribution Frame
MDU	Multi-Dwelling Unit
NFC	Near Field Communications
OLT	Optical Line Terminal
ONT	Optical Network Terminal
OTT	Over-the-Top
SCTE	Society of Cable Telecommunications Engineers
SSID	Service Set Identifier
Wi-Fi	802.11 Wireless Local Area Network

Bibliography & References

New England Institute of Technology. (2021, April 6). *What are the Different Types of Construction?* Retrieved from New England Institute of Technology: https://www.neit.edu/blog/what-are-the-different-types-of-construction

Parks Associates. (2021). *Future-Ready Broadband: Ubiquitous Connectivity for MDUs.* Retrieved from Parks Associates: https://www.parksassociates.com/products/whitepapers/mdu-wp2021

Parks Associates. (2021). *Supported Today's Connected Consumer.* Retrieved from Parks Associates: https://www.parksassociates.com/products/whitepapers/support-wp2021