Assuring Data Delivery from Critical IoT Devices

A Method to Create New Services and Mitigate Liability

A Technical Paper Prepared for SCTE•ISBE by

Michael Kloberdans
Principal Engineer
Charter Communications
14810 Grasslands Drive. Englewood, CO. 80112
(720) 518-2539
Michael.Kloberdans@Charter.com

Shlomo Ovadia
Director
Charter Communications
14810 Grasslands Drive. Englewood, CO. 80112
(720) 536-1686
Shlomo.Ovadia@Charter.com

Table of Contents

List of Figures

List of Tables

Introduction

Internet of Things (IoT) devices enable Machine-to-Machine (M2M) data transmissions where a sensor or appliance (machine) at a subscriber's residence collects and sends information to a different machine at another location, such as a mobile phone application, a gateway or even a data center. From that second machine, information is processed, made meaningful and available for human consumption. IoT devices mostly offer casual conveniences, such as changing the lighting color in the dining room or using voice commands to play a genre of music. Lately, a new class of IoT devices are emerging in homes and businesses that send critical and/or important messages such as personal healthcare data and industrial application data (e.g., factory temperature and pressure levels, etc.) to external processing or monitoring service providers.

IoT products have many categories: Gaming (Sifteo, console sensors), Security (Cameras, door/window sensors), Convenience (smart speakers, light bulbs, window shades, smart kitchen appliances), Monitoring (Plant soil moisture, pet food levels, lawn watering, automotive), Healthcare and others. Figure 1 shows the explosive growth of the Healthcare market, which is projected to reach $137 Billion in just two years [1].

Figure 2 shows, for example, the explosive growth of Smart Speaker devices in the US [2]. This category of IoT devices is interesting because they can control IoT devices as well as provide other services. Statistics from comScore reported that existing products such as Smart Speakers (Google Home, Amazon Echo, Apple HomePod, Sonos One, etc.) increased 50% to 18.7 Million US households in just three months between November 2017 and February 2018. This penetration growth reflects a broad acceptance of automation in US homes.

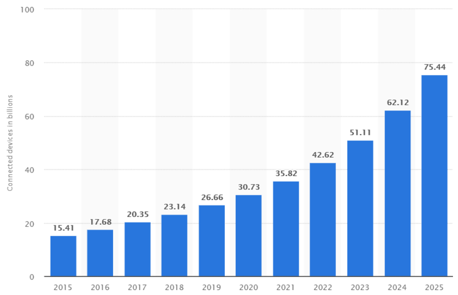


Figure 1 - Projected Number of Healthcare Devices Worldwide

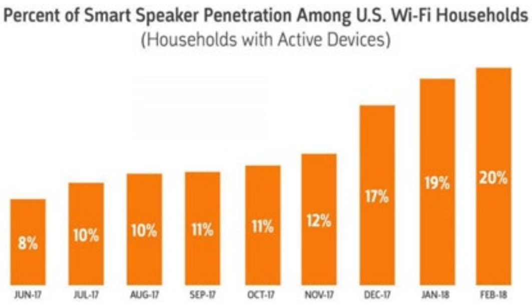


Figure 2 - Smart Speaker Penetration in US Homes

If vital data packets from these IoT devices are dropped anywhere in the network path between the IoT device and a processing and/or monitoring provider across the Internet, the necessary IoT function can be compromised, which in turn may as a consequence lead to property damage, health or safety problems. While critical IoT data devices use higher-layer data assurance protocols such as CoAP (Constrained Application Protocol) to acknowledge receipt of an IoT transmission, no receipt is possible if the source data fails to reach the processing/monitoring destination [1].

This paper provides one such solution with two main benefits:

1. A new service that alerts subscribers when expected, periodic data is missing.
2. Capability to identify where on the timeline packets are dropped in the Internet or other external network, which can prove helpful in ascertaining root-cause of outages.

The first of the two main benefits is alerting a subscriber when messages from critical and/or important IoT devices drop. This is a new proactive and potentially profitable customer service feature. For example, a medical blood oxygen sensor at the subscriber home sends a regularly-scheduled blood oxygen level information to a 3rd party monitoring company. If these regularly-scheduled data packets are no longer being received and transported through the Cable MSO network, the subscriber and the monitoring company are notified for corrective action to avoid a serious health consequence.

The second of the two main benefits is the ability to track packets in the Cable MSO networks to establish where and when on the transmission route packets were dropped, including drop events occurring after delivery to a non-MSO network such as the Internet. In addition to root cause identification, this information can mitigate liability issues by providing tracking visibility within the Cable MSO's systems of networks.

This paper is organized as follows. Section 1 presents the IoT data delivery network architecture and diagrams of IoT message flow through the data delivery network. Integration with existing Cable MSO transport protocols such as IPv4, IPv6, and MAP-T are explained. This section also discusses how IoT data loss is identified, and the triggers for required actions. Section 2 provides operational details of how the registered IoT device sends its critical data through various points of the data delivery network. Comparison with alternative methods to track critical IoT data through the Cable MSO network is discussed in the next section. The paper concludes with a summary of the key features of the assurance of critical data delivery through the Cable MSO network, and its benefits.

There are three clarifications listed here to give context to this paper: registration, generic naming, and SMB applications.

- Registration: Critical and/or important IoT device data must first be identified and registered for tracking and notification services to begin. Section 2 has details on this process, but for initial understanding, assume that the IoT device is pre-registered with the Cable MSO and its data is agreed as critical, important or 'of interest' as defined in section 2.4.4. In this paper, these IoT devices are referred to as 'Registered IoT Devices'. The alerting services and data tracking concepts are confined to these Registered IoT Devices only.

- Generic Names: The Cable MSO network device names used in this paper are intentionally generic because each Cable MSO has different network topologies and device function names. For example, there is no single egress point for a Cable MSO of any significant size. In general, the goal is to present concepts that can be applied to the network topologies of any Cable MSO.

- SMB Applications: While the focus in this paper is residential subscriber services, the same benefits and procedures apply equally to SMB markets although more formal implementation may be necessary to address the complexities of business demands and networks compared to residential needs.

Data Delivery Network Architecture & Operation

1. Data Delivery Network Architecture

1.1. IoT Packet/Header Flow in the Data Delivery Network Architecture

Figure 3depicts an architecture of physical devices and software entities in an IoT data delivery system for important and/or critical data from an IoT device. The key architecture components include an IoT device that sends data to a Home Gateway (HGW) where a unique ID is added. The Cable MSO premises contains an Access Network router that records HGW IoT packets and routes them through multiple network elements in the core network including a final egress router that both routes IoT data packets to a non-MSO network and sends IoT IPv6 headers to the IoT Data Repository database. Finally, these IoT data packets are received by a 3rd party monitoring provider. The blue text in the diagram below denotes actions that happen with an associated device and not a flow of packets or header copies. Generally, the device's packets use the UDP transport protocol which has no acknowledgement features. Also, while some IoT devices may use encryption for security purposes, an IPv6 header is always available which contains and tracks the unique ID.

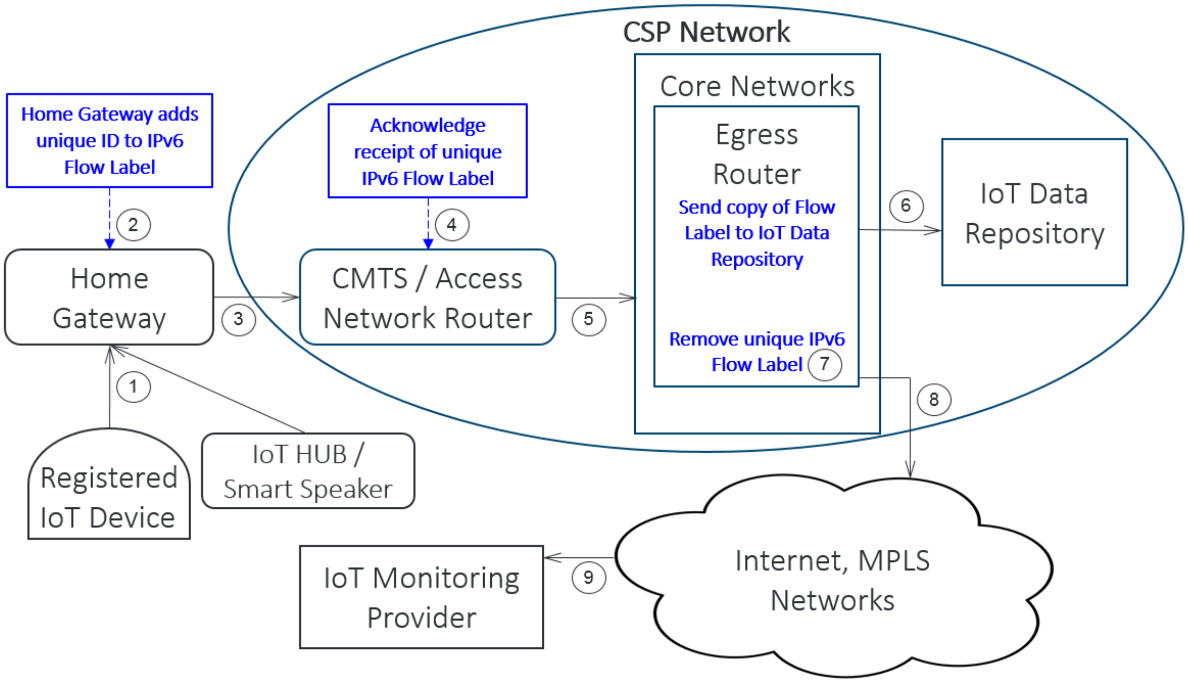
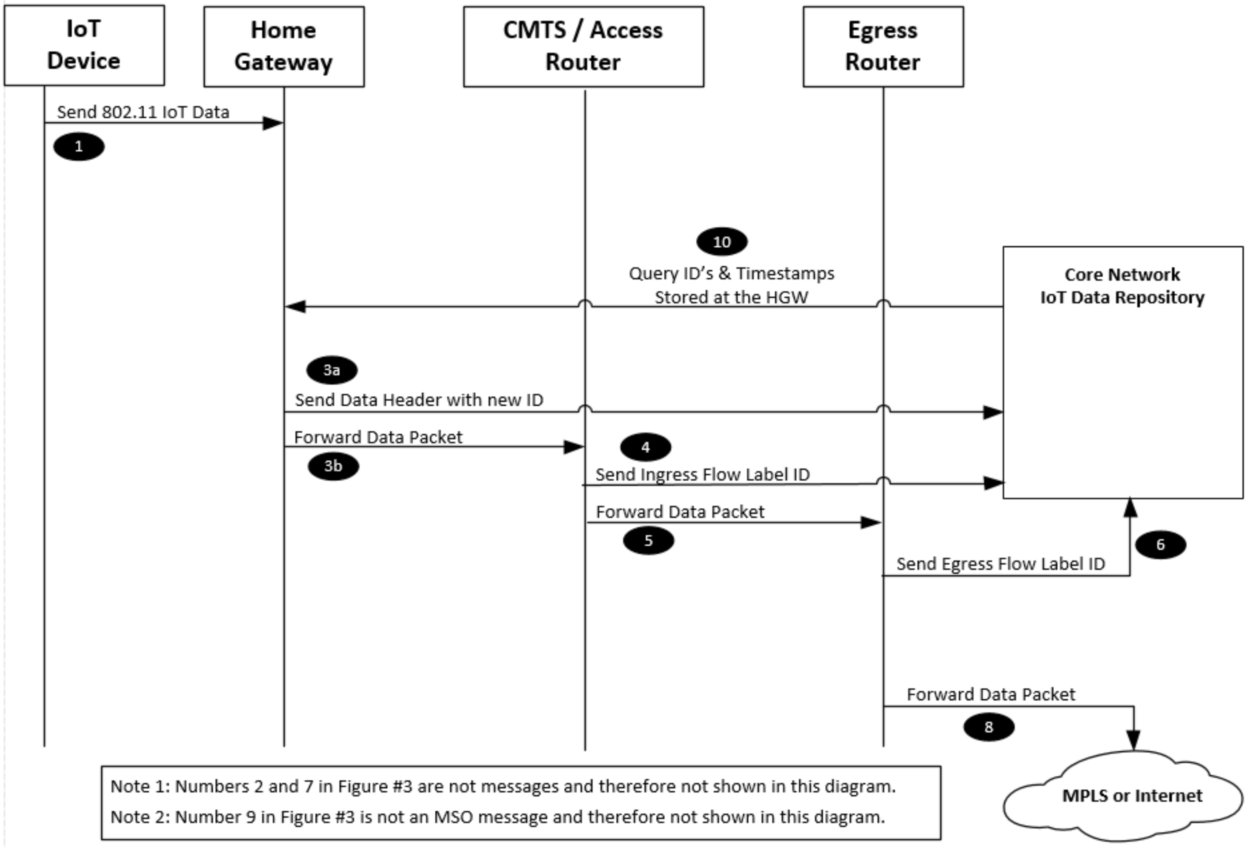

CSP Network
Core Networks
Egress Router
Send copy of Flow Label to IoT Data Repository
Remove unique IPv6 Flow Label
7
Home Gateway adds unique ID to IPv6 Flow Label
2
Acknowledge receipt of unique IPv6 Flow Label
4
Home Gateway
3
CMTS / Access Network Router
5
6
IoT Data Repository
8
1
Registered IoT Device
IoT HUB / Smart Speaker
IoT Monitoring Provider
9
Internet, MPLS Networks

Figure 3 - IoT Data Delivery Network Architecture: Major System Components.

Table 1 - IoT Data Packet Flow through the Data Delivery Network Architecture.

Step	Description of action at each architecture point
1	Registered IoT Device, Hub or Smart Speaker sends IPv4/IPv6 packet(s) to a Home Gateway (HGW).
2	The HGW adds a unique ID to the IPv6 Flow Label field that identifies the IoT device and the HGW.
3	The HGW sends the packets through a Cable Modem (CM) to an Access Network (AN) Router.
4	The AN Router sends a copy of the IoT data header and timestamp to an IoT data repository database.
5	The Access Network Router sends the data frame to the Cable MSO's core network infrastructure.
6	The Core Network (CN) Egress Router sends a copy of the IoT data header and timestamp to the same IoT data repository database as in step #4.
7	The CN Egress Router removes the unique ID from the IP packet.
8	The CN Egress Router sends the data frame to a non-MSO network such as the Internet.
9	The data packet is delivered to the final destination, such as an IoT Monitoring Provider.

Figure 4 shows the message flow diagram through the IoT data delivery network. The arrows indicate an action toward a destination, not necessarily a physical device. The message numbers shown in Figure 4 correspond to the numbers in the IoT data delivery network architecture shown in Figure 3.



Note 1: Numbers 2 and 7 in Figure #3 are not messages and therefore not shown in this diagram.
Note 2: Number 9 in Figure #3 is not an MSO message and therefore not shown in this diagram.

Figure 4 - Message Flow Diagram for IoT Data Delivery Network.

Table 2 - Message Flow Diagram through the Data Delivery Network Architecture.

Step	Message Flow Diagram Description
1	The Registered IoT Device, Hub or Smart Speaker sends one or more packets/frames to the HGW.
3a	The HGW creates a copy of the IoT IPv6 header, w/ID and sends it to the IoT Data Repository database
3b	The HGW forwards the complete IoT packet to the AN Router.
4	The AN Router sends a copy of the IoT IPv6 header to the IoT Data Repository database.
5	The AN Router forwards the complete IoT packet to the Core Network Egress Router.
6	The CN Egress Router sends a copy of the IoT IPv6 header to the IoT Data Repository database.
8	The CN Egress Router forwards the IoT packet using Non-MSO controlled networks onto the final destination.
10	Periodically, the IoT Data Repository database queries the HGW for all IoT messages sent. The period is defined for each device when creating the SLA and depends on the criticality of the device's data.

1.2. Key Architecture Points for Determining Data Loss

The basic IoT data delivery network architecture consists of three data collection points and a data assurance mechanism as shown in Figure 5. The data collection points are identified as points A, B and C representing message ingress at the home (A), Access Network ingress (B) and Core Network egress (C). Point D is the Data Assurance point.

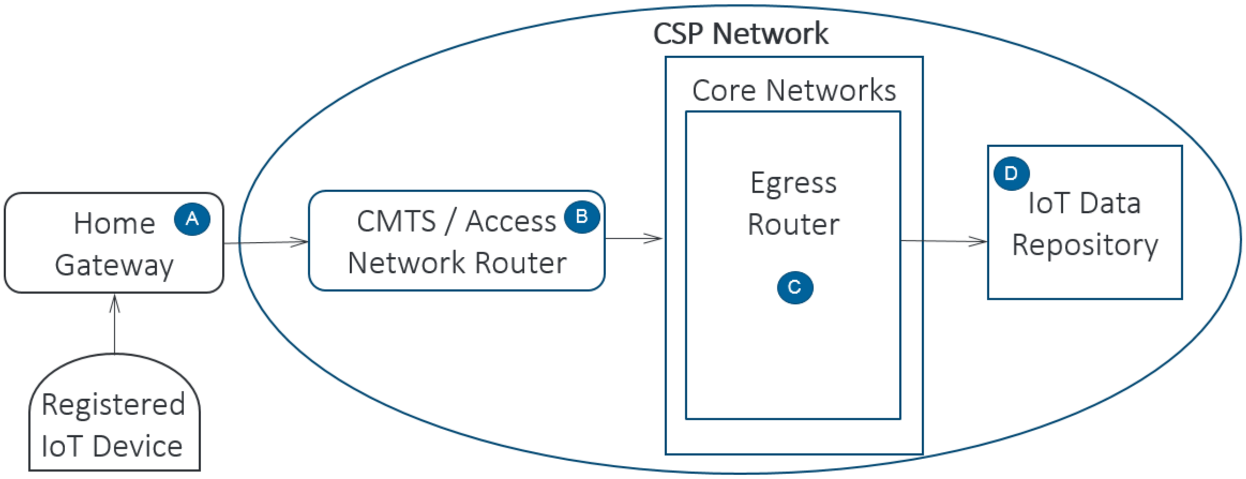


Figure 5 - IoT Data Delivery Network Architecture: Architecture Data Collection Points.

Table 3 - Network Collection and Assurance Points.

Network Point	Description	Function
A	Home Gateway (Home Ingress Point)	Data Collection Point
B	Access Network Router (AN Ingress Point)	Data Collection Point
C	Egress Router (Core Network Egress Point)	Data Collection Point
D	IoT Data Repository database	Data Assurance Point

Network Point A - Unless an IoT device uses cellular or other telecom protocols to communicate, the Cable MSO network is used. There are three common methods used to send IoT data to the HGW:

a. The HGW Access Point directly receives IoT wireless signals and forwards them to the Cable MSO Access Network.
b. The HGW Access Point converts wireless signals from an IoT device to a wired protocol and forwards that data to a wired IoT hub. IoT hub messages may then be forwarded back to the HGW for transport to the Cable MSO Access Network.
c. The IoT device directly communicates to an IoT hub or Smart Speaker (not shown in Figure 5). The hub or speaker then sends messages to the HGW to forward onto the Cable MSO Access Network.

The HGW copies the IoT frame header, adds a unique ID and a timestamp and then temporarily stores this information. The HGW information store is critical because the HGW is the only Cable MSO owned device that resides on the subscriber's LAN and is therefore the only point along the transmission route proximate to the subscriber at which originating IoT device transmissions can be recorded. The HGW then forwards the complete data packet (with the ID in the Flow Label field in the IPv6 header) onto the Access Network using normal routing mechanisms.

Network Point B - The Access Network Router is the entry point into the Cable MSO access network infrastructure which becomes another critical point for data collection because this point is the first time the data is fully 'inside' a totally Cable MSO controlled premises. Data from Registered IoT Devices are recognized at this point and like the HGW, a copy of the packet header is made and sent to the IoT Data Repository database. The IoT header copy is used to mark entrance into the Access Network.

Network Point C - The Egress Router is the final data collection point. Like the HGW and the Access Network Router, the Egress Router recognizes a packet from a Registered IoT Device by finding a non-zero value in the Flow Label header field, makes a copy of the packet header, and sends that header copy to the IoT Data Repository database. This header copy is used to mark the exit of the data packet from the Cable MSO-controlled network. The full data packet is delivered to the adjoining external (non-MSO) network associated at that point.

Network Point D - The IoT Data Repository database software agent periodically queries the HGW for a copy of the home premise IoT information store. The IoT Data Repository database compares the HGW entries with its own copy to verify that no Registered IoT Device data was lost between the HGW and the Access Network Router or the Egress router. All the Flow Label header copies with a matching ID are stored with their timestamps. This information is easily parsed to find any missing entries, and the identification of any missing entries triggers an action to find where the packet drop happened within the system of Cable MSO controlled networks (explained more fully in the section 2.4). This information can also be used to send an alert(s) to notify the subscriber of dropped packets or expected packets that were never received by the HGW.

1.3. Identifying Data Loss at Major Network Segments and Triggered Actions

Figure 6 depicts a simplified Cable MSO network showing the major network segments between points A, B, C and D, where loss can occur as identified by the red crosses. Table 4 shows a matrix of triggered actions as a result of data loss in each major network segment. It is important to determine data loss from a specific network area for accountability reasons and speedy repair. Depending on the IoT type and SLA, a subscriber notification of data loss may or may not be appropriate. Loss between any Subscriber's network device and the HGW is not part of the Cable MSO network unless HGW is malfunctioning. HGW errors are handled by existing policies and procedures and are outside this proposal.

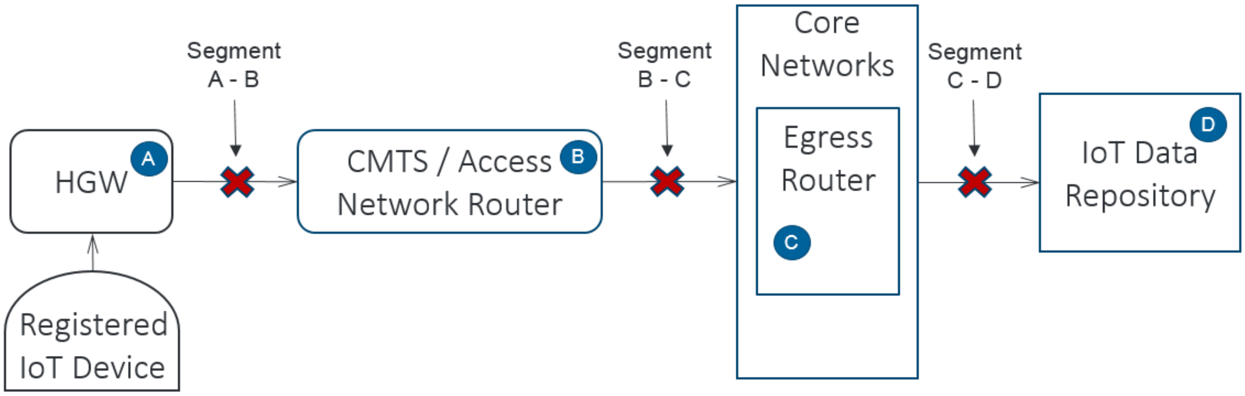


Figure 6 - IoT Data Delivery Network Architecture: Data Loss Segments.

Table 4 - Network Data Loss Action Matrix.

Network Segment	Location of Data Loss	Triggered Action
A - B	HGW to Access Network Router	Investigate path from HGW to AN Router
B - C	Access Network Router to Egress Router	Investigate path from AN Router to Egress Router
C - D	Egress Router to Repository	Investigate path from Egress Router to Repository

This proposal adds an additional capability from existing methods to find packet loss, and specifically from Registered IoT Devices only through the parsing of the database in the IoT Data Repository database.

Network Segment A – B:

Packet data loss on the Network Segment A – B can only be found from the comparison of the IoT Data Repository database to the HGW data store. As mentioned in the paragraph at Section 2.3, Network Point D, the IoT Data Repository database, periodically queries the HGW for a copy of the home premise IoT information store, and compares the HGW entries with its own copy to verify that no Registered IoT Device data was lost between the HGW and the Access Network Router.

Data loss can result from several sources:

- The HGW itself, such as a WAN interface defect that did not forward the data (or any data).
- An upstream Cable Modem defect, regardless of being an integrated or separate physical unit.
- A defect in the coax cabling, splitters or other components from the Cable Modem to the pedestal.
- Any component at the node, hub or headend, including the Access Network Router.

The general action triggered from loss in this network segment is to investigate the devices and network paths. More specifically, patterns are analyzed first to narrow the scope of investigation. An example is if one Registered IoT Device has no packets being sent, but other wireless devices on the customer's LAN have no issues with internet communications, the problem may be localized to the IoT device itself and the investigation should start with this device.

Network Segment B – C:

This segment can be complex, involving many separate networks and devices. Traditional network troubleshooting methods are used to find the issue and provide a fix. Most likely, non-IoT traffic is affected as well if transport problems are encountered on this network segment.

The general action triggered from loss in this network segment is to narrow the investigation scope, again, by using traditional troubleshooting methods.

Network Segment C – D:

More than one IoT Data Repository database may exist in actual implementations. The issues are either routing the data to a specific repository or finding the reason(s) that the repository won't accept or store the information.

The general action triggered from loss in this network segment is to determine if the problem source is network-based or is with the device(s) or database.

2. Operational Details

2.1. Registering Devices that Send Critical and/or Important Data

Before describing the packet flow details in this new architecture and in order that tracking and notification functionality can begin, critical and/or important IoT devices must first be identified and registered. The originating data source in this paper is the IoT device itself, but the treatment from critical and/or important data devices is not confined IoT devices only – any device can be registered for tracking and notification functionality. Thus, while any device can qualify, only IoT devices are mentioned for reasons of simplicity. Assume that the IoT source device of the previous section is pre-registered with the Cable MSO and its data is defined as critical or important and therefore tracking the data from this device is desired by both the Cable MSO and the subscriber. In this paper, critical and/or important IoT devices are referred to as a 'Registered IoT Device'. Alerting services and data tracking is confined to registered devices only. Both critical and important IoT data are tracked and monitored, but service actions vary depending on the degree of consequence severity as further explained in section 2.4.4. The registration process, use of a subscriber portal, automatic identification and other operational details are out of scope for this paper. Also, for purposes of this analysis unless an IoT device uses cellular or telecom protocols for communications, the assumption is made that they connect wirelessly to a HGW and use the Cable MSO's infrastructure for at least partial transport of their significant data to its final destination.

2.2. Identifying an IoT Device and Gateway Pair

Tracking data from critical and/or important IoT data devices at both the entry and exit points in a Cable MSO's network and then recording those results is foundational to this proposal. Identification includes the IoT device and the Home Gateway pair that sent critical and/or important IoT data to the Cable MSO network. A method to identify this paired information is needed, but anonymity is also needed for privacy concerns. Cable MSOs should track and record the movement of critical and/or important IoT data from the ingress to the egress points in their networks, but not record the data itself. Most subscribers' data devices still use the IPv4 protocol. A key feature of this architecture is to convert all IPv4 traffic to the IPv6 protocol at the Home Gateway. There are several methods that provide this conversion; MAP-T or MAP-E being the preferred method used by several of the largest Cable MSOs around the world.

The reason to use IPv6 is to repurpose a field in the header called the 'Flow Label'. The Flow Label field has a 20-bit length that defaults to all zeros. The HGW assigns an ID value to indicate the specific IoT device and gateway as a unique pair that is used to send the IoT data to the Cable MSO network.

A unique value to identify the IoT device/gateway pair can be derived using at least two methods:

1. Hashing – A hash value that fits within the 20-bit limit of the Flow Label header.
2. Mapping – A simple map of a registered IoT device and the subscriber's Home Gateway.

The ID calculation function is best performed by an OSS function, not the local HGW. This is done during the IoT Registration process, again, outside the scope of this paper. Both methods above ensure anonymity even if a Flow Label with an ID is accidentally exposed publicly or internally because the information cannot be traced to a subscriber or device without the mapping key or hash algorithm. Once an IoT/HGW pair has an assigned unique ID, that value is placed into the IPv6 Flow Label field of any packet transmitted from that device/HGW pair. The 20-bit Flow Label field is sufficient to provide enough unique IDs such that a single CMTS can serve over 40,000 subscribers where each subscriber can have up to 24 Registered IoT Devices. This ensures scalability for the near term but there are methods existing today that can be used to ensure ID extensibility with no practical limit, such as using IPv6 extension headers.

2.3. Tracking an IoT Device/Gateway Pair ID

As explained in section 1.3, there are three points at which the Unique ID (IoT device/Gateway pair information) is copied and sent to the IoT Data Repository database as described in Table 5:

Table 5 - Devices that Use the IPv6 Flow Label Header.

Device	Purpose
Home Gateway	Records IoT device data received at the home gateway
Access Network Router	Records IoT device data received at the Cable MSO access/core network
Cable MSO Egress Router	Records delivery of IoT device data from the Cable MSO egress point

2.4. Operational Details

2.4.1. Home Gateway Operational Details

The HGW identifies a data transmission from a Registered IoT Device, either directly or indirectly from an IoT hub or another device. If the HGW doesn't have an integrated cable modem, a separate Cable MSO provided cable modem encapsulates the Ethernet frame for transport between the cable modem and the CMTS (or similar) using DOCSIS protocols. In this paper, we assume that the cable modem is integrated into the HGW device. The HGW then completes the following steps:

1. Identifies packets from a Registered IoT Device using its MAC address or other identifier.
2. Converts from a wireless protocol such as IEEE 802.11ac to a wired protocol such as IEEE 802.3 (Ethernet).
3. Converts IoT device data from IPv4 packets to IPv6 if needed.
4. Assigns a predetermined, unique ID value (IoT and gateway pair) into the IPv6 Flow Label header field.
5. Copies that IPv6 header, applies a timestamp and:
    a. Stores this header information in non-volatile memory on the gateway.
    b. Forwards this same header information to the IoT Data Repository database.

6. Forwards the complete packet with the modified IPv6 Flow Label to the Access Network Router.
7. Waits for a periodic query from the IoT Data Repository database (or other actor performing this verification step). After acknowledgement that data was successfully transported from the HGW to the IoT Data Repository database, the HGW data stored in step 5a above is reset and ready to be used for new entries.

2.4.2. Access Network Router Operational Details

After the IoT data packet exits the HGW, (or the cable modem or the ONU), it traverses the Cable MSO access network, and then terminates at the Access Network Router. At this point in the access network, the following operations are completed:

1. Identifies in-scope packets by detecting a non-zero IPv6 Flow Label value in the IPv6 header.
2. Copies the IPv6 header, applies a timestamp and:
    a. Stores this header information in non-volatile memory on the Access Network Router.
    b. Forwards this same header information to the IoT Data Repository database.
3. Forwards the complete packet with the modified IPv6 Flow Label using standard routing procedures throughout the Cable MSO's network infrastructure to the Network Egress Router.
4. Waits for a periodic query from the IoT Data Repository database (or other actor performing this verification step). After acknowledgement that data was successfully transported from the Access Network Router to the IoT Data Repository database, the Access Network Router data stored in step 2a above is reset and ready to be used for new entries.

2.4.3. Egress Network Router Operational Details

Standard Cable MSO routing transports critical important and /or important IoT data from the Cable MSO Access Network Router which eventually terminates to a router at the edge of the Cable MSO network. At this point in the core network, packets egress from the Cable MSO controlled networks and complete a hand-off to a non-MSO network such as the Internet or MPLS network. The following operations are completed at the Cable MSO Egress Router:

1. Identifies packets of interest by detecting a non-zero IPv6 Flow Label value in the IPv6 header.
2. Copies the IPv6 header, applies a timestamp and:
    a. Stores this header information in non-volatile memory on the Egress Router.
    b. Forwards this same header information to the IoT Data Repository database.
3. If the external non-MSO network uses these IP protocols:
    a. IPv6 - then reset the IPv6 Flow Label in the header of the complete packet to a value of all zeros and forward to the adjoining network.
    b. IPv4 - then convert the IP protocol of the packet from IPv6 to IPv4 and forward to the adjoining network.
4. Forwards the complete packets to the adjoining non-MSO network using current procedures for normal operation.

2.4.4. IoT Data Repository database Operational Details

The IoT Data Repository database contains copies of the IPv6 Flow Label headers and timestamps from three network points that have handled the packets issued from registered IoT device transmissions; the HGW, the Access Network Router, and the Egress Router. This is described in sections 1.3 and 2.3. The purpose of the IoT Data Repository database is to store the following records of the IoT data transmissions:

- Initially generated and received at the Home Gateway
- Received at the Access Network Router
- Received at the Egress Router
- Successfully handed off to the non-MSO adjoining network

A typical IoT Data Repository database structure example is shown in Table 6 where the IoT/HGW ID values are hexadecimal and time is represented as Unix Epoch Time values:

Table 6 – Example of IoT Data Repository database entries.

Entry	IoT/HGW ID	HGW Time	Access Network Time	Egress Router Time
1	B0301	1 531 179 199.501	Not Available	1 531 179 200.691
2	40A4E	1 531 179 200.519	Not Available	Not Available
3	665B2	1 531 179 198.637	1 531 179 198.660	1 531 179 199.112
4	665B2	1 531 179 798.243	1 531 179 798.651	1 531 179 799.145
5	665B2	Not Available	Not Available	Not Available

Any missing timestamp entry in the IoT Data Repository database indicates missing data at that collection point; HGW, AN, or Egress router. If a notification SLA is active, a lack of entries from an IoT device indicates missing data and triggers one or more alerts to the subscriber. Therefore, this table serves as a missing data detection point that triggers proactive alerting, which in turn can provide the customer with notice of the possibility their IoT devices are not receiving signal and cannot function as intended.

An example of missing data and corresponding action responses from Table 6 is now described:

Entry #1 has no timestamp value delivered from the AN collection point, but has a value from the Egress router collection point. This missing data in inconsequential and no action is taken because the IoT data was received into and egressed from the Cable MSO’s system of networks.

Entry #2 is concerning because it represents data loss within the network segment from the HGW and the AN collection points. A triggered action would include investigating these network elements:

- If data is missing from many subscribers terminating at the same AN router, that AN router, AN router interface or physical media attaching to the AN router interface are investigated. As previously stated, this type of data loss most likely affects all data from all sources and not just IoT data. Therefore, other alarms and procedures would most likely detect and address this outage.
- If data is missing from one subscriber only, faulty components could include the HGW itself, the cabling between the HGW and the CM (if they are separate physical devices), the Coax/Fiber cabling between the CM and the pedestal and every component between the pedestal and the AN.

Entries 3 - 5 are an example of missing data from an IoT device sending regular and periodic messages once every 10-minutes. An SLA is in place where proactive alert notifications are sent if the IoT device doesn’t send data as expected within the stated time period. Entries 3 & 4 represent normal and expected messages from the IoT device. Entry #5 is expected, but failed to be recorded at any collection-point.

Alert notifications would be sent to the subscriber and perhaps a 3rd party monitoring agency as defined in the SLA.

Registered IoT Device data are classified as one of three different types: Critical, Important or 'of interest' and might have corresponding SLA service packages labeled as Gold, Silver and Bronze. Cable MSO triggered actions such as notifications will vary depending on the class of data and SLA agreement. For example, missing data from a medical pulse monitor can be critical with only a few minutes to respond before health is threatened or even death results. This data class is 'critical' and results in immediate notifications to the subscriber and also health professionals and emergency providers. By contrast, an important message would be a power outage to an IoT-monitored large freezer could result in only an informative notification to the subscriber. The contents in the freezer may be unaffected for many hours during a power outage. This important information class is higher than 'of interest' but not critical. The class titled 'of Interest' is data that is not critical or important, but the subscriber wants Cable MSO monitoring and notification messages sent.

Lastly, the IoT Data Repository database can be archived as desired or rewritten after a suitable time period as the Cable MSO desires. Database reliability is met through common practices for redundant server/storage that are used today.

Comparison with Alternative Methods

Complex solutions exist today to track data, video and voice, specifically Lawful Intercept (LI) [4] for legal monitoring purposes, however, this level of effort is expensive to administer and may be affected by governing restrictions under multiple industry standards [5] [6] and those initiated by a judicial/administrative legal order.

LI begins as an unexpected legal order from the state or federal government judicial or administrative branch. This is therefore an unplanned and reactive request. A subscriber's IP address is first identified, and then manual administration is performed to mirror a copy of those IP Packets (Voice, Video and Data) to the government agency that made the demand. Manual administration is again needed remove the packet mirroring. The Cable MSO are subject to restrictions under law regarding copying, redirecting or storing these packets for purposes other than securing, maintaining, and otherwise delivering the underlying services. Using the LI solution for IoT devices would result in significant architectural changes and also copying and storing the entire packet, including sensitive payload data which makes this a heavyweight solution and introduces many privacy problems that would need to be solved.

By contrast, the data delivery assurance method described in this paper plans data tracking in advance for each Registered IoT Device and is governed by subscriber SLAs. It is lightweight in comparison to LI because only packet headers are stored and it is also fully controlled by the Cable MSO. It also enables new subscriber services to pay for the setup and operational costs and become profitable. Because only IPv6 headers are copied and stored, there are no privacy issues which results in benefits without risks.

Table 7 - Comparison between the LI and IoT Data Delivery Assurance Methods

Method Name	Benefits	Costs
IoT Data Delivery Assurance Method	• Relatively simple to implement • Relatively low implementation cost • Generates on-going subscriptionss • Enables Cable MSOs to introduce new services • Controlled proactive agreement w/subscriber and 3rd party vendors (SLA) • Minimizes potential liability issues due to data packet loss • Allows deeper Cable MSO integration and involvement with subscriber's IoT devices	• Requires the installation and maintenance of additional network functionality: • HGW, AN & CN header copies and timestamps • IoT Data Repository database
Lawful Intercept (LI) Method	• None for the Cable MSO	• Complex administration • Privacy issues • Reactive service • Costly • No Cable MSO benefit • Not designed for tracking data • Create data storage

Conclusion

Explosive growth of IoT devices is expected to continue well into the next decade (e.g., Figure 1 and Figure 2). Subscribers have already embraced the use of IoT devices as conveniences, and are accepting and using a new class of IoT applications to monitor and transmit critical and/or important data in various areas such as personal health, safety, etc. If the IoT device's critical and/or important data is dropped anywhere in the network between the IoT device and the Cable MSO egress router or the 3rd party monitoring provider across the Internet, then there can be significant consequences to the subscriber.

In this paper, a novel and simple data delivery assurance method was presented to resolve this problem. The method is based on first registering the IoT device and the HGW pair in the Cable MSO database. The registered IoT IPv6 label header, which has a unique ID, is then used to track the IoT data packet flow through the network. In addition, the registered IoT IPv6 label header is timestamped at various key network elements as the packet is transmitted from the HGW to the Cable MSO egress router and stored at the IoT data repository database. If an IoT data packet is lost in the Cable MSO network, a matrix of triggered actions is enacted at the identified network segment. Depending on the IoT type, data type and SLA, the subscriber may receive a notification for the loss of IoT data packets. The IPv6 header reuse is a transparent function to both the IoT devices and the network elements beyond the Cable MSO network infrastructure. This ensures that non-MSO devices and network elements function normally when this solution is applied.

There is great potential for new service offerings associated with the use of IoT devices that transmit critical and/or important data. Furthermore, strong partnerships with external 3rd party monitoring agencies can result in proactive data loss notifications that are sent to both the subscriber and the monitoring agency for faster resolution and to lessen the impact of missing data. Liability concerns associated with unfounded fault attribution can be mitigated, if not eliminated through the use of this tracking method.

Alternative methods such as the LI method are costly, complicated to administer, and are not designed for tracking the IoT data packets through the Cable MSO network. In contrast, the data delivery assurance method is relatively simple to implement and administer, and can even prove profitable depending how the Cable MSO may offer such additional functionality to the subscriber or other parties, such as health monitors.

Wireless cellular technology is currently being used in many cases for IoT data transport. However, cellular carriers do not have the tracking and alerting capabilities or the granular focus to support a per IoT device SLA contract. Adopting the IoT Data Delivery Assurance method will potentially enable the Cable MSOs to compete with the wireless cellular carriers as an alternative low-cost solution to guarantee the delivery of critical and/or important IoT data from the home or the business to the 3rd party monitoring companies.

Abbreviations

AN	Access Network
AP	Access Point
CM	Cable Modem
CN	Core Network
CMTS	Cable Modem Termination System
CoAP	Constrained Application Protocol
DOCSIS	Data Over Cable Service Interface Specification
EU	End User
HGW	Home Gateway
ID	Identification
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IoT	Internet of Things
LI	Lawful Intercept
M2M	Machine to Machine
MAC	Media Access Control
MAP-T	Mapping Address and Port using Translation
MAP-E	Mapping Address and Port using Encapsulation
MPLS	Multi-Protocol Label Switching
MSO	Multiple System Operators
OSS	Operations Support Systems
ONU	Optical Network Unit
SCTE	Society of Cable Telecommunications Engineers
SLA	Service Level Agreement
US	United States

Bibliography & References

[1] Internet Engineering Task Force (IETF) RFC7252, the Constrained Application Protocol (June, 2014).

[2] IoT Number of Connected Devices, Statista. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

[3] Smart Speaker Penetration among US Wi-Fi households, Forbes. https://www.forbes.com/sites/johnkoetsier/2018/04/11/smart-speaker-penetration-just-exploded-50-in-3-short-months/#744e086b4fbf

[4] Lawful Intercept Overview, Cisco. https://www.cisco.com/c/en/us/td/docs/routers/10000/10008/feature/guides/lawful_intercept/10LIovr.html

[5] Lawfully Authorized Electronic Surveillance, TIA/EIA/J-STD-025A. http://cryptome.org/espy/TR45-jstd025a.pdf

[6] PacketCable Electronic Surveillance Delivery Function to Collection Function Specification, PKT-SP-ES-DCI-I02-070925. https://www.forbes.com/sites/johnkoetsier/2018/04/11/smart-speaker-penetration-just-exploded-50-in-3-short-months/#744e086b4fbf