Does Matter overcome security issues of implemented communication standards?

Michael Geiger

A thesis submitted for the degree of MSc Cyber Security

Department of Computing

University of Essex

September 2023

Abstract

The smart home IoT market is characterised by a rapid increase in areas of application and the associated use of these devices by consumers. However, a large number of communication standards are currently used in this area, resulting in interoperability problems. In addition, the established standards have security gaps which, in the event of inappropriate implementation, lead to opportunities for hackers to attack. To meet these challenges, the Matter communication standard was developed, which is intended to eliminate interoperability problems, simplify the development of new devices by manufacturers and at the same time promises a high level of security for consumers. Matter builds on the already existing Wi-Fi, Bluetooth and Thread standards. However, since there are known vulnerabilities in these standards, it is necessary to question how secure Matter is. To investigate this, the research question is asked: Does Matter overcome security issues of implemented communication standards? To answer the research question, experiments were carried out which investigate known attack possibilities with regard to the Wi-Fi and Bluetooth standards used in Matter. In a quantitative investigation, hacking tests against Matter as well as alternative networks have been carried out to allow comparisons between Matter and the corresponding network standard used by Matter. The results obtained show that Matter is able to meaningfully meet the required standards according to their respective strengths. Furthermore, some security features such as the comparison of certificates and measures related to data integrity could be determined. However, it was also possible to find vulnerabilities with regard to de-authentication attacks in the WPA2 security protocol used under Wi-Fi. From this it can be concluded that Matter is not adequately protected using security protocols older than WPA3, which increases the threat of downgrading attacks, in which attacker deliberately exploit vulnerabilities of older security standards.

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgment, the work presented is entirely my own.

Frankfurt am Main, 06.09.2023

Michael Geiger

Acknowledgements

I would like to express my sincere gratitude to my advisors, Douglas Millward and Dr. Cathryn Peoples, for their invaluable guidance and support throughout my master's program. Their expertise and encouragement helped me to complete this research and write this thesis.

Table of contents

List of Tables and Figures

Tables:

Figures:

1. Introduction

The rapid development of the Internet of Things (IoT) has produced an ever-increasing number of networked devices that are used in almost all areas of life (Pedhadiya et al., 2019). However, this rapidly growing number of IoT devices has also brought with it increased complexity and heterogeneity of the communication standards used (Augusto-Gonzalez et al., 2019). As a result, many of these standards are vulnerable to security threats, as well as interoperability and scalability issues (Touqeer et al., 2021).

IoT devices in the field of smart homes have the primary purpose of making everyday life easier for users. Smart devices such as smart electric shutters or heaters can also increase energy efficiency, and smart door locks and surveillance cameras can contribute to the security of the residents of a smart home. However, malicious access and intervention in such IoT devices can also result in serious dangers. For example, users have already been falsely warned of the impact of a ballistic missile via their smart home device (Hollister, 2019). In another case, smart home residents heard voices from a camera implemented on the network and the hacker took control of the smart thermostat, increasing the indoor temperature to 32°C (Maher, 2019).

Spoofing attacks can be used to spy on victims, which not only compromises their right to privacy, but also information about the behaviour and routines of the victims can be collected, which could be misused for burglaries, social engineering attacks or extortion (Allhoff & Henschke, 2018). Denial of service attacks can render devices inoperable, so that functions of the smart home fail and physical damage can occur. However, the protection provided by IoT security devices can also be significantly impaired. Man-in-the-middle attacks can not only be misused for espionage. With replay attacks, devices connected to the smart home network can be controlled remotely, which not only impairs their functions, but can also be used against the legitimate user. These examples represent only a few practical consequences resulting from the theory of possible threats to smart homes.

One promising attempt to address these challenges is the Matter communications standard, formerly known as Project CHIP, developed by leading technology companies and industry partners (CSA, N.D.a).

1.1 Ethical considerations in IoT

Malicious manipulation of IoT devices can cause them to stop working or malfunction, resulting in device function failure or being used for malicious actions that can result in both financial and physical damage to devices or even people. The psychological component of a successful attack on the smart home should also not be underestimated. Many people perceive their own home as a safe and private place. The psychological consequences of a hacking attack on the victim's home can be the same as those associated with a physical burglary (Brantly, 2017). These include the feeling of insecurity in one's own home, powerlessness and helplessness, a permanent feeling of anxiety, stress and sleep disorders (Wollinger et al., 2014).

In addition to the individual dangers that exist as a consequence of a hacking attack on IoT devices in the smart home network, threats on a macroscopic level must also be taken into account. According to Statista (2022), there were 8.6 billion IoT devices in 2019 and 13.14 billion in 2022 in use. This large number of Internet-enabled devices can pose an enormous risk potential if they are not adequately secured, as they can be misused for Distributed Denial of Service (DDoS) attacks. The consequences of such attacks can be the collapse of parts of the Internet. The fact that these devices pose a serious threat was shown by the Mirai botnet, which blocked access to over 1200 websites for almost a day in 2016 as a result of a DDoS attack using corrupted IoT devices (Zhang et al., 2020). It is important to note that this attack involved *only* 100,000 malicious endpoints (Woolf, 2016).

Manufacturers of IoT devices therefore have a responsibility towards users and society as a whole to adequately protect these devices from malicious manipulation. However, it must be taken into account that security applications in IoT devices are in some cases more difficult to integrate than in conventional Internet-enabled devices, since IoT devices are limited in their technology. A restricted size, limited performance capacities and the need for a low power consumption mean that conventional protective measures cannot always be implemented (Hameed & Alomary, 2019). It should also be noted that the economics of manufacturing IoT devices contribute to the vulnerability of these devices. A key goal of many companies in the manufacture of IoT devices is to develop cost-effective devices. However, the development and implementation of security features is associated with a cost factor that is often neglected (Holz, 2022). Also, in many cases, IoT devices are used for long periods of time without being replaced. Without appropriate updates, these devices may not be protected against newly discovered vulnerabilities (Chantzis et al., 2021).

Matter has been proposed as a mitigation against these threats by standardising the communication standard and the associated regulations. Standardisation is intended to reduce cost factors in the development of security components and strengthen long-term resilience (CSA, N.D.a). With these promises, Matter is therefore responsible for coordinating sufficient security standards among the manufacturers and for protecting end users and society from threats arising by Matter devices.

1.2 Research question and validation approach

This scientific work focuses on the central question of whether the Matter communication standard is able to overcome the vulnerabilities of Bluetooth sniffing, de-authentication attacks, as well as replay attacks. The aim is to examine how Matter is structured, to what extent common security features have been taken into account by the standards used and are operating under Matter, and what the resilience of Matter networks is in relation to hacking attacks.

To carry out the tests within the scope of this project, networks of Matter-capable devices were created on the basis of the publicly available reference implementations and the experiments were executed on them. Test networks were created based on the respective communication standard and the experiments were also carried out on them to compare Matter to the standards used by Matter. This should on the one hand confirm the basic functioning of the hacking attacks and on the other hand create a basis for comparison to validate results and to compare Matter with other standards.

1.3 Structure of the project

This thesis comprises the following structure. In chapter 2 a literature review of the most important advantages and disadvantages as well as the dominant vulnerabilities of common IoT communication standards in use is carried out. Chapter 3 covers the Matter communication standard, its goals and principles, as well as the structure and security aspects relating to the standard. In chapter 4 the methodology of the project is discussed and then in chapter 5 the procedure of the experiments and their results are presented. Finally, in Chapter 6, a discussion of the test results obtained and the associated conclusions took place.

2. Literature Review

2.1 Smart home ecosystems

Smart home ecosystems represent the network on the basis of which communication standards implement data transmission and control of devices (Dasgupta et al., 2019). In such an ecosystem, individual IoT devices are interconnected in a cohesive topology that enables communication between the devices via defined standards. A large number of devices with different functions can be located in a smart home IoT. These include, for example, power and light switches, door locks, roller shutters, sensors, control devices, as well as end devices of everyday life such as household appliances and telecommunications and entertainment devices.

In principle, different communication standards can be used in an ecosystem, but they must be compatible with each other to ensure the interoperability of devices. Due to the respective advantages and disadvantages of the individual communication standards, none of the currently used standards can be identified as a universal application solution of IoT in the smart home area. Several standards are therefore often implemented in parallel in an ecosystem to use the application-related strengths (Tightiz & Yang, 2020).

2.2 Communication standards in the smart home area

To understand the problems of commonly used communication standards, some of the dominant communication standards in the IoT smart home area, Wi-Fi, Bluetooth Low Energy, Thread, Zigbee and MQTT are examined for their strengths and weaknesses.

A distinctive feature of communication standards is the differentiation between wired and wireless standards. While wired standards like Ethernet require a physical transport medium in the form of a cable, wireless standards use radio frequencies to transmit data. In this project, however, only wireless standards are discussed, as these constitute the fundamental innovation of Matter (CSA, 2021). To highlight the problems of the currently used communication standards, the most common wireless standards in the IoT smart home area are considered in the sections 2.2.1 – 2.2.5.

2.2.1 Wi-Fi

One of the most used wireless communication standards is IEEE-802.11, also known as Wi-Fi (IEEE Standards Association, 2021). Through the Wi-Fi Alliance certification process, manufacturers can prove that their devices meet the guidelines of the standard and can therefore communicate with other Wi-Fi enabled devices (Wi-Fi Alliance, 2010). Consumers can thus easily see whether a device is compatible with their network. The Wi-Fi standard describes uniform communication using a wireless local area network (WLAN). WLAN is the umbrella term for Wi-Fi certified devices, so from a technical point of view there are no significant differences (Badman & Parmenter, 2020). As a result, IoT Wi-Fi devices in the smart home area can be easily embedded into the existing WLAN network, making it user-friendly (Danbatta & Varol, 2019).

In the IEEE 802.11 standard, the first two layers of the OSI model, physical layer and data link layer, are defined more precisely (IEEE Standards Association, 2021). Protocols such as IP and TCP/UDP can be used based on the layers of the Wi-Fi standard to define the network and transport layers. Most Wi-Fi networks are built in a star topology in which each device is connected to a central connection node and all communication takes place via this point. Communication as well as authentication in the network takes place via a central access point (AP), which is mainly implemented by a router and connects the network to the Internet (Ding et al., 2018). However, because of the mesh technology, it is also possible to form a network with several APs. This can increase the range as well as the area coverage (Kirichek et al., 2020). Compared to other standards, the Wi-Fi communication standard is primarily characterised by its high data transmission rate of up to 11.2 Gbit/s (Nguyen et al., 2019). On the other hand, this is accompanied by high power consumption of the devices. In summary, the use of Wi-Fi devices is particularly recommended in areas of application that allow a direct connection to the power grid.

Wi-Fi security is achieved through Wi-Fi Protected Access Version 3 (WPA3), although older versions of WPA are no longer considered secure (Alhamry & Elmedany, 2022). WPA3 includes secure authentication in the network, as well as encryption of data traffic (IEEE Standards Association, 2021). However, it should be noted that WPA3 also has security vulnerabilities (Baray & Ojha, 2021). With the help of the Dragonfly handshake, communication is established which supports both elliptic curve cryptography and finite field cryptography (Appel & Guenther, 2020). Thus, WPA3 offers a better security measure than

the previous versions, but still has some vulnerabilities that can be exploited if implemented improperly (Vanhoef & Piessens, 2018).

2.2.2 Bluetooth Low Energy

Another communication standard used in the smart home sector is Bluetooth Low Energy (BLE). The standard, designed for short distances, was developed by the Bluetooth Special Interest Group (SIG) (Bluetooth SIG, N.D.). Like Wi-Fi, BLE operates on the 2.4 GHz frequency band and is characterised by lower power consumption, but has lower data transmission rates of up to 2 Mbit/s (Bluetooth SIG, 2023). Figure 1 shows the BLE architecture based on the OSI reference model.

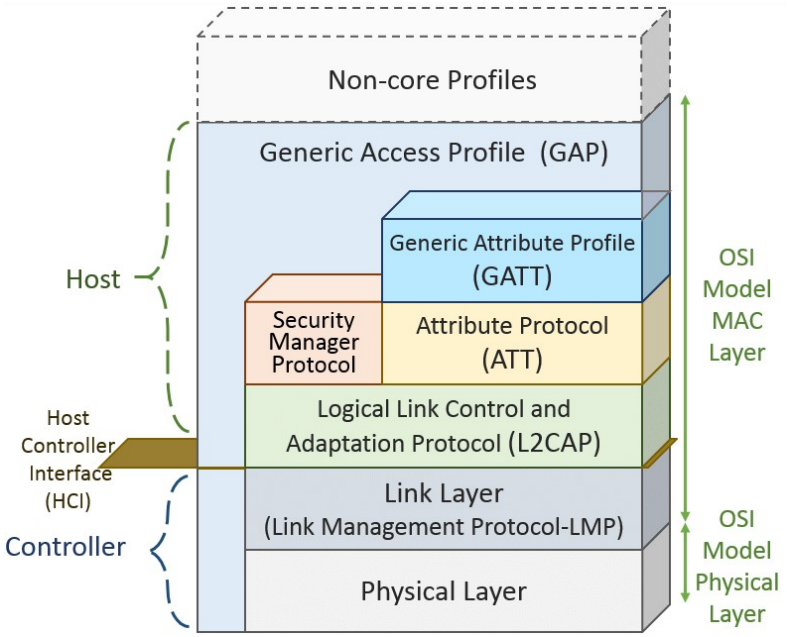


Figure 1: BLE protocol stack (Oliveira et al., 2019)

It can be stated that, in contrast to Wi-Fi, the complete BLE protocol stack differs depending on the application (Bluetooth SIG, 2023; Gomez et al., 2012). Another advantage of BLE can be found in the easy implementation of devices in the network. The advertiser opens the connection and regularly sends out broadcast packets, making it visible to connectable devices. The scanner in turn searches for possible connection partners and can initialise the connection setup. A password is not required for the coupling, but there is the possibility that the advertiser must first confirm the incoming connection manually in order to set up a connection so that no unwanted couplings are created.

Once a connection has been established, the sending party is called ‘Active’ and the receiving party is called ‘Standby’. Since Bluetooth 4.1, these roles are no longer static, so that mesh networks are also possible with BLE (Darroudi & Gomez, 2017). With the introduction of Bluetooth 4.2, support for the transmission of IPv6 packets was also developed.

From a security point of view, however, the Bluetooth standard has conceptual vulnerabilities. The authentication and encryption of existing connections is implemented with the Advanced Encryption Standard (AES) algorithm in combination with cipher block changing message authentication code (CCM) mode, which is considered to be a strong encryption method (Mewada et al., 2016). However, the connection establishment is not secure, so that without appropriate precautions in the application layer, all messages can be read until the coupling is completed (Darroudi & Gomez, 2017).

2.2.3 Thread

The Thread communication standard, developed by the Thread Group, was published in 2014 and is thus the newest of the standards examined (Randewich, 2014). Thread was developed to provide a wireless connection between low power devices, using the 2.4 GHz spectrum and is based on IEEE 802.15.4 radio technology (Thread Group, N.D.). Suitable for both small and large networks, the standard communicates via IPv6 (Rzepecki et al., 2018). The comparison of Thread with the OSI model in Figure 2 shows that the physical layer and the data link layer are adopted from the IEEE 802.15.4 standard.

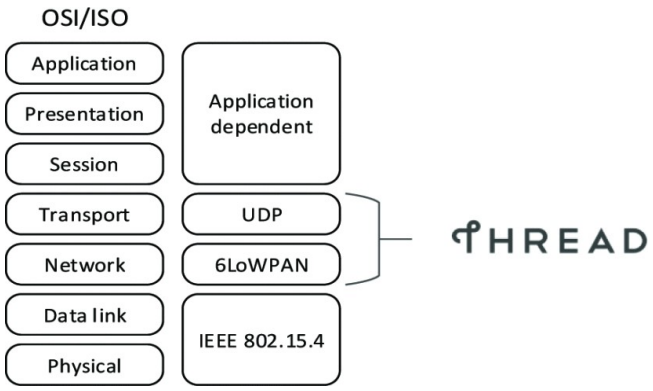


Figure 2: Thread comparison with OSI (Rzepecki & Ryba, 2019)

On the network layer, Thread uses the 6LoWPAN network protocol, which allows the transmission of IPv6 packets over the IEEE 802.15.4 standard and enables the mesh topology (Unwala et al., 2018). An advantage resulting from the application for resource-poor devices

is the flexible size of the packet header, which, in contrast to the fixed header sizes in the IPv4 protocol, enables a lower network load. However, this is also necessary because of the low data transfer rate of 250 kbp/s (Samuel, 2016). Thread uses UDP for the transport layer, whereas the layers above it are defined by the application and are therefore not part of the standard.

Border routers are required as gateways to the Thread network to enable Internet capability and the control of Thread devices via end devices that cannot communicate directly via Thread (Unwala et al., 2018). A second border router can be used for improved reliability. Thread routers are solely responsible for communication within a Thread network and can dynamically change routes to maintain reliability in the event of failure, with the centre of the network always being a leader who registers the other routers in the network and manages their responsibilities (Herrero, 2022).

With Thread, the security of the communication is realised with a network-wide key. As with BLE, the AES-CCM method is used for encryption, while the key exchange is based on the Diffie-Hellmann method (Marksteiner et al., 2017; Akestoridis et al., 2022). However, since there is only one key in a network, the compromise of one device is sufficient to be able to decrypt all devices and their communication, which means that insecurely designed IoT devices pose a serious threat to the entire network.

2.2.4 Zigbee

Another common communication standard in the smart home environment is Zigbee, which was specially developed for the requirements of the IoT. Zigbee was developed and standardised by the Zigbee Alliance, now Connectivity Standards Alliance, a global consortium of companies (CSA, N.D.b). The protocol stack of Zigbee is shown in Figure 3.

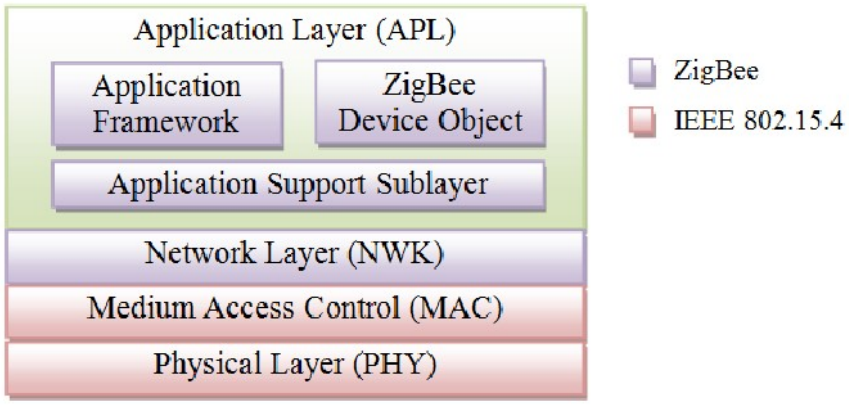


Figure 3: Zigbee protocol stack (Sung et al., 2010)

Like Thread, the standard is based on the IEEE 802.15.4 standard, which specifies the physical and data link layers and is defined by the Zigbee standard from the network layer onwards (Zigbee Alliance, 2016). This enables ZigBee-enabled devices from different manufacturers to be compatible with one another.

Another advantage of Zigbee is its low energy consumption. Zigbee devices can be battery powered and have long battery life making them ideal for IoT applications using batteries (Alobaidy et al., 2020). This is made possible by minimising data transmission. Devices based on the Zigbee standard can spend most of their time in a standby state to extend battery life. For transmission, the standard can communicate on a frequency of 2.4 GHz as well as on sub 1 GHz frequency bands (Zigbee Alliance, 2016).

The ability to self-organise is also an advantage of Zigbee. Zigbee devices can automatically connect to a network and form a mesh network (Adi et al., 2021). This improves the resilience and reliability of the network as there are alternate communication paths in case a device fails or the signal is weak. Furthermore, the simple design based on the IEEE 802.15.4 standard, low hardware requirements and the Zigbee open source model enable comparatively low manufacturing costs (Long & Miao, 2019).

A disadvantage of Zigbee is the limited bandwidth. The standard was mainly developed for low data rate applications, such as sensor data or control information, so the maximum data transmission rate is 250 Kbit/s (CSA, N.D.c). Another disadvantage is the limited range of Zigbee. Although Zigbee devices can achieve greater range over mesh networks, the single range of a Zigbee device is limited compared to other wireless standards such as Wi-Fi or Bluetooth (Adi et al., 2021). Furthermore, Zigbee devices do not support communication with computing devices, since in most cases they do not have a Zigbee module. Therefore, a bridge

is required for the smart home with Zigbee, which takes over the distribution of the commands.

With Zigbee, communication is encrypted using the AES-CCM method (Zohourian et al., 2023). However, this is not used on the data link layer as defined in the IEEE 802.15.4 standard, but on the network layer. In this way, routing information can be read by forwarding entities (Khanji et al., 2019). As a result, attackers could use side channel attacks to eavesdrop on the distribution of the keys and thus decrypt the encryption.

2.2.5 MQTT

Message Queuing Telemetry Transport (MQTT) is an open source communications standard specifically designed for transferring messages between devices with limited bandwidth and high latency. It was developed by IBM in 1999 and handed over to the Eclipse Foundation as an open standard in 2010 as part of the MQTT project (Yuan, 2021). MQTT is widely used in the Internet of Things (IoT) to enable efficient and reliable communication between devices and applications. The standard is based on a publish-subscribe model, in which messages are sent from a publisher to one or more subscribers (International Business Machines Corporation & Eurotech, 2015). This model allows for loose coupling between the devices and applications involved. MQTT uses a lightweight protocol over TCP/IP that incurs little overhead and minimises the resource load on the devices involved.

A major advantage of MQTT is its efficiency and scalability. As MQTT is a lightweight standard, it requires less bandwidth and storage compared to other communication protocols (Soni & Makwana, 2017). In addition, MQTT supports a variety of topologies, with multiple publishers and subscribers. This enables scalable and flexible communication between many devices and applications. Another advantage of MQTT is its reliability. It supports message receipt with acknowledgment to ensure messages were successfully transmitted (Atmoko et al., 2017). This reliability is particularly important in applications where critical information is transmitted.

MQTT also offers high flexibility and interoperability. It is platform independent and can be implemented on different operating systems and devices (Bender et al., 2021). There are also a large number of MQTT brokers who act as intermediaries between publishers and subscribers. These brokers can run on different systems and enable communication between

devices from different manufacturers. This enables seamless integration and collaboration between devices.

Despite these advantages, MQTT also has some disadvantages. A disadvantage is the limited support for complex data structures. MQTT mainly supports the exchange of simple messages transmitted as strings or binary data (Soni & Makwana, 2017). MQTT is less suitable for applications that require complex data structures or extensive metadata. Furthermore, MQTT does not have any standardised security functions (Chen et al., 2020). Security must be implemented through additional mechanisms such as Transport Layer Security (TLS) or Virtual Private Networks (VPNs) to ensure secure communication. This can mean additional implementation effort and increase complexity.

2.3 Challenges of interoperability between communication standards

Inadequate compatibility can mean that certain functions of the devices cannot be used. This problem is referred to as a lack of interoperability between smart home devices and manufacturers (Noura et al., 2019). ISO (2015) defines interoperability as, "*capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units*".

A central cause of interoperability problems results from the large number of device types, which have different functions and thus address different data structures (El Jaouhari et al., 2019). In many communication standards, profiles are predefined at the application level, which classify the most important functions of a device type (Valtchev et al., 2002). This has the advantage that not every manufacturer has to implement every function of a device individually and can focus on innovations. However, in terms of interoperability, this property of the standards poses a challenge. In order for all messages in a network to be translated from one protocol to another, gateways must know all the application profiles used (Phan & Kim, 2020). With an increasing number of manufacturers and IoT devices, it is no longer practical for gateway manufacturers to implement this large number of application profiles. If a gateway is not able to translate the data of a device on the application level, it follows that not all functions of the device can be used properly.

To solve the interoperability problems, one approach could be a universal communication standard (Hazra, et al., 2021). This relieves the gateways of a manageable number of application profiles. However, a comparison of existing communication standards in IoT shows that each standard has its own advantages and disadvantages, so that the corresponding standards are currently used depending on the area of application and operating system used (Samuel, 2016). Another possible solution is the development of a gateway that is able to dynamically add application profiles from the manufacturer's servers to its own database (Aloi et al., 2016; Phan & Kim, 2020). It must be assumed here that the application profiles are made freely available by the manufacturers. Taking into account the large number of manufacturers and IoT devices, this approach represents a major organisational and political effort.

The initiative to develop a uniform IoT framework was initiated by the Open Interconnectivity Foundation (OCF) in 2016 (OFC, N.D.) OFC aims to develop a publicly accessible framework to counteract fragmentation in the IoT landscape. The framework sets guidelines for interoperability between different standards in a network. In order to ensure interoperability, it is recommended to use IPv6 at the network layer level, which applies to each of the considered communication standards (OCF, 2022). However, the largest and leading manufacturers have also taken on the challenge of interoperability problems and have been developing the new communication standard Matter in cooperation under the leadership of the Connectivity Standard Alliance (CSA) since 2020.

2.4 Threats of IoT in smart home

IoT devices have limiting factors in terms of size and power consumption due to their areas of application. This limitation of performance capacity is accompanied by technical limitations of possible implementations of security mechanisms (Gupta, 2019). However, the economical manufacture of IoT devices also contributes to the vulnerability of IoT systems (Chantzis et al., 2021). Many companies place an emphasis on device cost effectiveness, which in turn makes device security an undesirable expense. This also means that buyers are usually not sufficiently informed about the secure configuration of the devices (Emami-Naeini et al., 2019). It should also be considered that IoT systems can often be used for several decades without having to be replaced (Chantzis et al., 2021). Devices without Internet access in

particular are therefore subject to the increasing risk that these devices are not secured against newly discovered vulnerabilities.

Numerous attacks on IoT networks and smart home ecosystems have been discovered and published in recent years (Dorobantu & Halunga, 2020). It is possible to classify these attacks into known patterns. One type of attack is signal jamming, where the goal is to disrupt the transmission between two devices, thereby affecting the availability of the system (Alhammadi & Zaboon, 2022). This is typically achieved by sending interfering signals, which means that the devices can no longer receive relevant messages from the radio traffic.

Another common type of attack is the replay attack, in which an attacker tries to read messages between two devices and then sends them to the original recipient. It is not necessary for the attacker to crack the encryption mechanisms used in order to manipulate the behaviour of the target device (Marksteiner et al., 2017). While battery-powered IoT devices can lead to a targeted increase in power consumption and thus massively decrease battery lifetime, such attacks can lead to serious health risks in the context of medical IoT devices (Butt et al., 2019).

In setting tampering attacks, attackers try to change the configuration of the target device (Chantzis et al., 2021). For example, this can result in malicious server requests being accepted or all incoming requests being blocked. In addition, IoT devices are often vulnerable to hardware integrity attacks. These are attacks that involve physical access to the device hardware, such as malicious code injection through an unprotected USB port (Abomhara & Køien 2015).

Since IoT systems usually include a large number of devices, attackers can try to imitate legitimate devices via node cloning attacks (Mogbil et al., 2020). In this way, an attacker could imitate the control unit in a network and thereby gain access to the entire network. All attacks in which communication between devices in a network is intercepted can be summarised under the term security and privacy breaches (Chantizis et al., 2021). The attackers monitor network communication and, if necessary, try to circumvent the encryption of the messages in order to read out relevant information. In addition, the risk of human error always remains. This includes, for example, social engineering or phishing attacks, where an attacker can gain control of the system (Ali & Award, 2018).

The use of IoT standards and frameworks, such as those provided by Matter, offer manufacturers support, as they already implement many security mechanisms and thus

simplify and accelerate development. However, this support can also lead to a false perception of security. There is an assumption that a most widely used framework or communication standard already has sufficient security measures when in reality there may be fundamental security problems (Gupta, 2019).

3. The Matter communication standard

The communication standard Matter, originally developed under the name Project Connected Home over IP (CHIP), was designed by CSA (2021) in cooperation with leading IoT manufacturers for use in the smart home environment. The project was announced in 2019 and development started in 2020. The implementation-first approach was followed during the development process, so that the reference implementation was provided before the technical specifications were published (Heater, 2019). The final version of the reference implementation became available as open source and the certification process started in October 2022 (CSA N.D.a).

The primary focus in the development of the Matter standard was to solve the interoperability problems in the field of IoT smart home networks. Furthermore, security has been pursued by Matter as a fundamental principle (CSA, 2022a). It is also intended to simplify the usability of the devices and to support the development process of new devices.

3.1 Structure of Matter

The structure of Matter is shown in Figure 4.

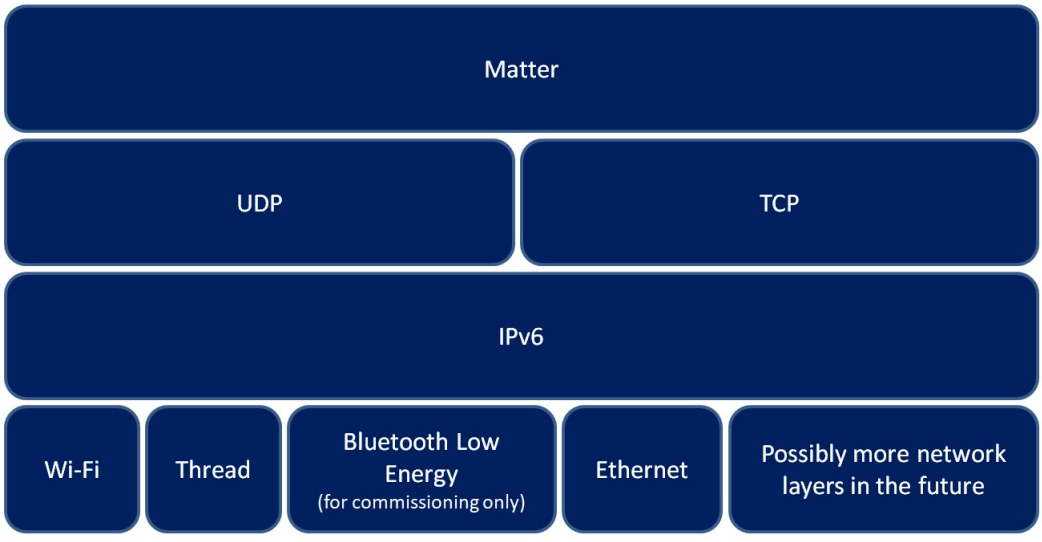


Figure 4: Structure of Matter (revised according CSA, 2022a)

At the lowest level, the Matter communication standard is based on data transmission via Wi-Fi, Thread, BLE and Ethernet. It should be noted that BLE is only used to authorise new devices as it allows for a simple pairing process (CSA, 2022b). While the transmission of data

is realised via Ethernet for wired connections, there is a choice between Wi-Fi and Thread for wireless connections.

All participating standards on the network layer support IPv6, which ensures the basis of Matter interoperability. The network communication protocols TCP and UDP, which are typical for IP-based stacks, are used on the transport layer (Kumar & Rai, 2012). In this way, connection-oriented as well as connectionless applications can be realised. Figure 5 shows the splitting of the architecture into seven components.

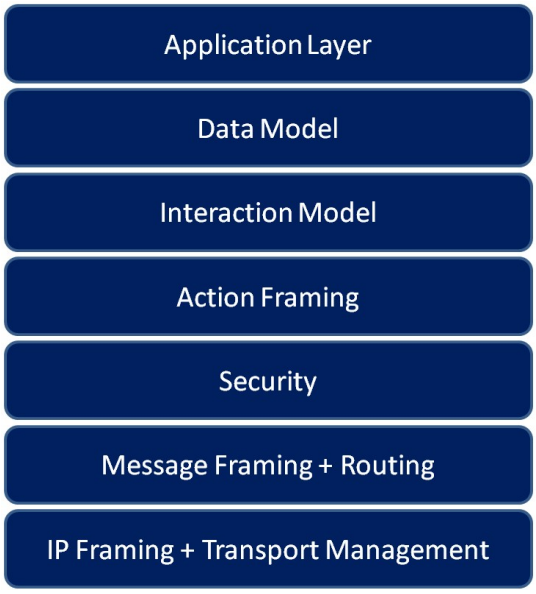


Figure 5: Architecture of the Matter framework (revised according CSA, 2023)

The application layer represents the highest level of logic within the framework. Simple functions such as commands to switch on or off and colour characteristics of a light bulb are implemented on this level. The data model describes the structure through which the data of an application can be accessed. The interaction model determines which commands can be used to interact with the device based on the defined elements of the data model. This includes, for example, how data can be read or changed on the device. The action framing layer transforms the incoming interaction commands into a binary format for transmission. Security mechanisms are used on the security layer to encrypt and authenticate the data for the sender and recipient. The data is then organised into packets and provided with routing information and headers. Finally, the packets are forwarded to the transport management layer, where the IP management of the data takes place.

3.2 Network topology by Matter

A central goal of Matter is to improve interoperability in the smart home area. Due to the compatibility of several communication standards, a Matter network can take on different topologies, with the primary topology being a mesh network. Figure 6 shows various possible applications of a Matter network.

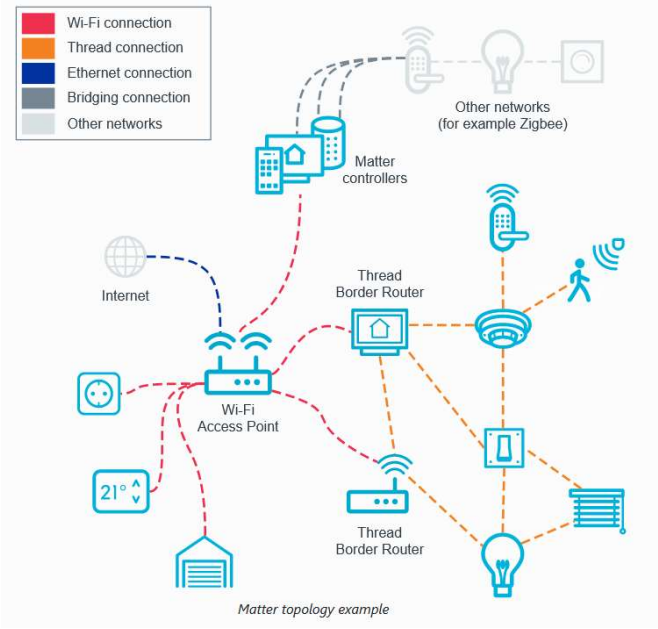


Figure 6: Matter network topology (Nordic, 2023)

The centre of the network is the connection between the Wi-Fi router and control devices (CSA, 2021). Smartphones, tablets or smart speakers are suitable as control devices, which enable the user to interact with the network and the devices connected to it. BLE is used to integrate new devices into the network, as this allows for a simple initial connection (Asadullah & Ullah, 2017). If the Bluetooth connection is successful, the device is implemented in the Wi-Fi network through secure transmission of the access information. Finally, the Bluetooth connection will be disconnected and is no longer used for further communication between the devices (CSA, 2022c).

The implementation of Thread devices in the Matter network is made possible by border routers, which connect the subnets and realise the translation between Wi-Fi and Thread. In addition, Matter Bridge Devices enable the embedding of other communication standards such as Z-Wave or Zigbee (CSA, 2023). The Matter Bridge functions in the same way as a border router does when embedding threads in a Matter network.

3.3 Security principles and considerations by Matter

The goal when developing Matter was to implement the security of the standard using five principles (CSA, 2022a). A representation of these principles can be found in Table 1.

Table 1: Matter security principles (CSA, 2022 a)

Principle	Explanation
Comprehensive	Layered approach
Strong	Well-tested standard cryptographic algorithms such as ECC NIST P256 & AES-CCM-128
Easy	Improve ease of use not decrease it
Resilient	Protect, Detect and Recover
Agile	With crypto-flexibility in mind to address new developments and threats.

The first principle builds on the comprehensive, layered structure of Matter. The security mechanisms are not dependent on the protocols on which Matter is based. All functions relevant to the security of communication are provided in the open source framework (CSA, 2022c). This should enable device manufacturers to build on the reference implementations without having to consider additional security mechanisms. However, it should be questioned to what extent the implementation of communication standards for which vulnerabilities are known can be securely transferred to Matter without posing a security risk.

The second principle relates to the use of proven and strong cryptographic algorithms and encryption techniques. As with BLE and Thread, AES is also used in CCM mode to maintain secrecy, with Matter using 128-bit keys. Furthermore, the hash method SHA-256 is used to support integrity, which is currently classified as secure (NIST, 2022). The setup of a session is based on the use of x.509 certificates, which are used to authorise a device to participate in the network (CSA, 2022a). Device certificates can be checked using the Distributed Compliance Ledger (DCL) technology (CSA, 2022c). DCL provides a blockchain-based platform on which manufacturers can upload product information for their products without the risk of the data being manipulated (Higginbotham, 2021). This data includes the device ID, the manufacturer ID and meta data, such as references to a device's update sources. This is to ensure that anyone can verify the integrity and certification of a device.

Another principle of Matter is that it is easy to use for both manufacturers and users. Through freely accessible reference implementations, manufacturers can adopt the security measures

designed and specified by Matter (CSA, 2022b). According to Matter, when it comes to security, users do not have to consider the security aspect at all when implementing and using their devices due to the security functions implemented in the standard (CSA, 2022a).

The resilience of Matter represents the fourth principle. In order to realise this, there are often several ways to carry out an action. An example of this can be found in establishing a session. If a session already exists but is unexpectedly interrupted, Matter first attempts to re-establish the connection using an abbreviated recovery protocol to minimise disruption to communication (CSA, 2022a). However, if this attempt fails, the session is re-established using the full protocol. Precautions against the most common DoS attacks and checking firmware integrity are mentioned as further resilience measures (CSA, 2022b).

Finally, the fifth principle deals with the agility of the standard. Due to the modular structure of Matter, it should be possible in the future to exchange the cryptographic methods and protocols used without having to completely revise the present specification. This should allow Matter to be flexibly adapted to future developments in the field of cryptography and quickly close new security threats (CSA, 2022a).

3.4 Identity attribution of Matter devices

Device identity supports security in already existing mechanisms, since before a device is added to a new network, its origin and firmware can be checked (CSA, 2022c). Each device's identity is assured by a chain of certificates, which is shown in Figure 7.

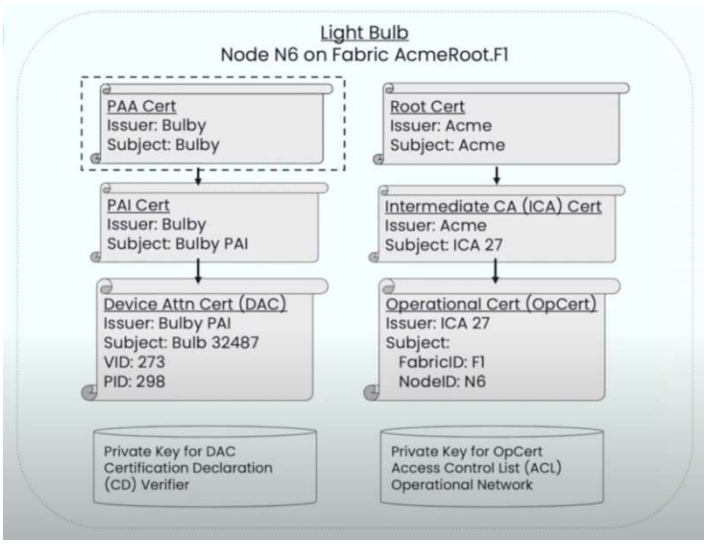


Figure 7: Certificate chain example (CSA, 2022b)

Each device has a Device Attestation Certificate (DAC) that contains information such as device ID, vendor ID, device name, public key, and a reference to a parent certificate to verify the authenticity of the DAC. This chain goes all the way to the root certificate, also known as the Product Attestation Authority (PAA) certificate, which is held by the manufacturer and serves as a source of trust. This infrastructure is similar to the public key infrastructure used in the web environment by Internet browsers and by Matter to authenticate devices and ensures that only certified devices can access the network (Clutterbuck, 2010).

In the factory state, the private key for checking the certificate, a declaration of the certificate and a verification of the declaration are also stored on the device. This declaration confirms that the device has been tested and certified with the specified vendor ID and device ID. If the device is successfully integrated into the network, an additional certificate is created that describes the identity in the network. This operational certificate contains a unique designation of the device in the network, the network designation, the public key of the device and a reference to the parent certificate. Similarly, the chain of certificates goes back to the root certificate, which is trusted by all devices in the network. The original DAC is preserved so that the device can be added to another network in the future (CSA, 2022b).

4. Methodology

According to Matter's developers, it is claimed that "This industry-unifying standard is a promise of reliable and secure connectivity" (CSA, N.D.a). In particular, the users of the new communication standard are relieved of responsibility. CSA (2022a) states that “Customers buying Matter devices will not have to think about security: it is just there”.

These statements can be rated as particularly interesting since Matter is currently based on the communication standards Wi-Fi, BLE and Thread and these each have known vulnerabilities (Bernal et al., 2018; CVE, N.D.a; CVE, N.D.b). This raises the question of whether Matter is able to overcome the vulnerabilities of Bluetooth sniffing, de-authentication attacks and replay attacks of the communication standards on which the new standard is based.

4.1 Type of research and approach

To investigate this question, experiments have been carried out in a Matter network, which are based on known and dominant vulnerabilities in the Wi-Fi and BLE communication standards. Therefore, the present project can be classified as an analytical project. An analytical approach makes sense in this context, since known vulnerabilities in the old communication standards have already been examined in depth, so that penetration testing procedures that have already been developed and tested for these standards can be transferred to the new standard Matter.

The project approach follows deductive reasoning, since the experiments are intended to evaluate CSA's claim regarding the security of Matter and thus whether central security aspects based on known vulnerabilities have been taken into account. A quantitative data collection was carried out, based on a comparison of the results of known penetration testing methods of established communication standards and the new Matter standard. This made it possible to determine in direct correlation whether a threat can also be applied to Matter by using the accuracy metric.

Various communication networks were set up to collect data. These were a Matter network, as well as the control networks of the Wi-Fi and BLE standards. With the help of the control networks, penetration testing procedures were carried out with regard to explicit vulnerabilities, so that comparative data were available for the subsequent experiments. The tests were then carried out in a Matter network using the same procedure. Based on the

control experiments, it was then possible to validate whether Matter demonstrates better security with regard to the selected penetration tests.

4.2 Specific research details

To create and carry out the experiments, Matter networks were created, which consisted of the three components AP, control device (hub) and Matter device as shown in Figure 8. A home WiFi router that supports the WiFi standards 802.11g/n/ac/w was used as the AP for the Matter network. This formed the basis of the network.

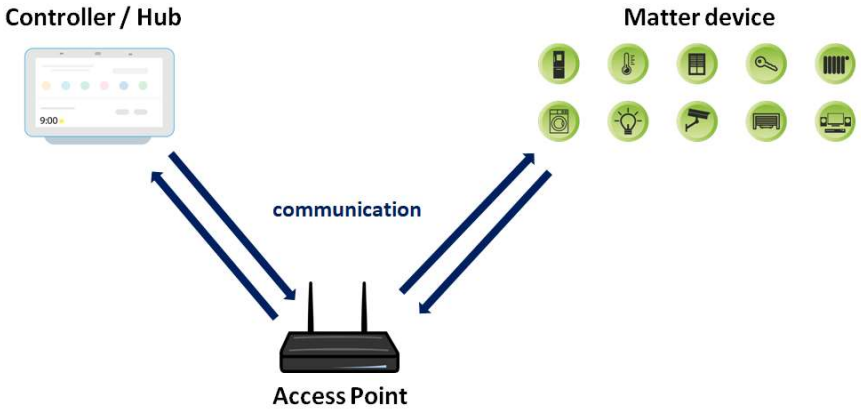


Figure 8: Matter network architecture diagram

The ESP32-S3-DevKitC-1 microcontroller was used as the Matter device (Espressif Systems, 2023). Matter supports ESP32 microcontrollers and states in their Github repository that the ESP32-S3 series can be used for the applications all-cluster-app and lighting-app (Patil et al., 2023). The microcontroller used has a built-in LED, which can be controlled via Matter. It should be noted that in addition to the ESP32 controller, Matter also supports a large number of other device types. However, the choice fell on an ESP32 microcontroller, as this offers a cost-effective way to create Matter-compatible devices.

Various devices were tested and used as control devices for the Matter-based network. These include the devices Google Nest Hub (2nd generation) and iPad (3rd generation), which are explicitly intended as a hub, as well as a computer running the Ubuntu 22.04 TLS operating system, which can be used as a test hub using the chip tool (Kajor et al., 2023).

Appropriate devices corresponding to the experiments were used as comparison networks. A smartphone (Huawei P30) and an AppleWatch were used as part of the Bluetooth testing. Furthermore, the nRF52840 semiconductor was used to carry out the BLE sniffing, which enables the detection of BLE packets via Wireshark (Nordic, 2023; Wireshark Foundation, N.D.). Thus, the collected packets could be analysed using Wireshark.

For the de-authentication attack, an Ubuntu 22.04 TLS computer (acer Aspire V7 series ZRQ), as well as the home Wi-Fi router and an AP provided by a smartphone (Huawei P30) were used as a test network. The execution of the de-authentication attack was realised by the DSTIKE Deauther MiNi V3 (DSTIKE, N.D.).

The comparison test of the replay attack was carried out using a client-server setup between two Ubuntu 22.04 TLS computers. As in the Matter network experiment, Wireshark was used, which allowed the data packets sent to be recorded. Furthermore, an attempt was made to remotely record the packets sent via the Wi-Fi network using the corresponding Wi-Fi dongles tp-link TL-WN722N and BrosTrend AC1200. The Python-based Scapy tool (version 2.5.0) was used to execute the replay attack, which is able to read, manipulate and resend the information packets collected by Wireshark (Scapy, N.D).

4.3 Risk assessment

Regarding possible challenges and risks related to this project, some aspects had to be considered to guarantee the success of the project.

First of all, it had to be taken into account that although Matter was in a published version at the start of the project, there were regular changes to the open source Matter repository over the course of the project. The risk had to be taken into account that by the time the project was completed, the outcomes resulting from the project could no longer be transferred to the updated version of Matter and would therefore be outdated. To minimise this risk, the data collection processes were recorded in detail so that the experiments can be repeated shortly before the project is completed using the latest version of the Matter Repository, so that changes in the test results can be adjusted accordingly. However, it cannot be guaranteed that the research results will be comparable with the newest version of Matter after the project has been completed.

Another risk is that the data collected could have only limited meaning in relation to the research question. Matter is a comparatively new communication standard, so there is currently hardly any scientific literature focusing on the security of Matter that can be used for comparison. The project was therefore subject to the risk that sufficient validation was not possible on the basis of the experiments. In order to counteract this risk, procedures and penetration testing of vulnerabilities were chosen which are typical for the communication standards compatible with Matter. This guaranteed as a minimum goal that an assessment could be made as to whether the successful hacking attempts of the other standards were also successful with Matter.

Furthermore, the cost factor represented another risk for this project. Devices had to be purchased to carry out the experiments. It had to be taken into account that the planned experiments were also feasible from a financial point of view. A risk would have emanated from tests that would have included Thread in addition to the Wi-Fi and BLE communication standards, since a compatible infrastructure would have had to be created for this using a border router. Since appropriate devices such as a network router or BLE-capable end devices such as smartphones were available for the examination of Wi-Fi and BLE, the cost factor could be significantly reduced.

5. Test execution and results

As part of this project, two of the central communication standards on which Matter is based were examined for dominant vulnerabilities and corresponding attacks were carried out to analyse the security of Matter. In the following, the Bluetooth and Wi-Fi standards are examined with regard to selected attack scenarios and exemplary tests are carried out against these standards as well as Matter.

5.1 Hacking attacks against Bluetooth

Bluetooth is one of the most widely used communication protocols in everyday use (Herrero, 2022). However, it should be noted that the standard has some vulnerabilities that affect all Bluetooth versions. A serious vulnerability is that when establishing a connection between two devices, only the slave device needs to be authenticated, but not the master device, which initiates the authentication. It follows that access to the control device means full control over the Bluetooth devices connected to the network. It also allows an unauthorised person to connect to the device before the owner and thus have control of the device until the owner physically intervenes to discard the connection. This is favoured by the fact that Bluetooth devices do not have a limited period for connection detection. This enables Bluetooth devices to be examined for their properties and possible vulnerabilities.

5.1.1 Bluetooth sniffing execution and results

The tool hcitool was used to carry out an initial probing of the Bluetooth devices in the test environment (Miller & Estrella, 2018). Using hcitool, available Bluetooth devices can be detected and at the same time the devices can be subdivided with regard to the Bluetooth and BLE protocols. Figure 9 shows the found Bluetooth and BLE devices.

```
michael@michael-testenv:~$ hcitool scan
Scanning ...
        1C:B7:96:38:8F:67       Smartphone
michael@michael-testenv:~$ hcitool inq
Inquiring ...
        1C:B7:96:38:8F:67       clock offset: 0x7718    class: 0x5a020c
michael@michael-testenv:~$ sudo hcitool lescan
[sudo] password for michael:
LE Scan ...
00:C3:F4:F7:4A:8F (unknown)
EA:B7:87:B4:1F:76 (unknown)
79:91:C4:41:C9:C0 (unknown)
79:91:C4:41:C9:C0 (unknown)
BC:14:85:B8:E3:27 (unknown)
D3:6C:D4:6B:A3:71 (unknown)
D3:6C:D4:6B:A3:71 (unknown)
^Cmichael@michael-testenv:~$
```

Figure 9: hcitool Bluetooth and BLE device scan

The test shows that the Bluetooth device named for the test 'Smartphone' was found by the command ‘hcitool scan’ and the MAC address could be determined. Further information such as the clock offset and the class of the Bluetooth device could be determined using the inquire remote devices command ‘hcitool inq’. However, this command was unsuccessful with BLE devices. The ‘hcitool lescan’ command displays all BLE devices in the area, but the respective names cannot be determined. Repeated tests of the lescan command also revealed that the Matter device displayed a new MAC address after switching it off and on again. Figure 10 shows repeated lescans with multiple reboots of the Matter device.

```
michael@michael-testenv:~$ sudo hcitool lescan
LE Scan ...
6F:4A:B6:FE:C8:B8 (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
00:C3:F4:F7:4A:8F (unknown)
F2:A4:82:14:D5:59 (unknown)
E5:F7:26:CB:F9:2F (unknown)
E5:F7:26:CB:F9:2F (unknown)
^Cmichael@michael-testenv:~$ sudo hcitool lescan
LE Scan ...
00:C3:F4:F7:4A:8F (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
F2:A4:82:14:D5:59 (unknown)
F9:25:23:3A:C2:2F (unknown)
F9:25:23:3A:C2:2F (unknown)
^Cmichael@michael-testenv:~$ sudo hcitool lescan
LE Scan ...
00:C3:F4:F7:4A:8F (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
F2:A4:82:14:D5:59 (unknown)
D5:62:7F:6B:83:12 (unknown)
D5:62:7F:6B:83:12 (unknown)
^Cmichael@michael-testenv:~$ sudo hcitool lescan
LE Scan ...
00:C3:F4:F7:4A:8F (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
6F:4A:B6:FE:C8:B8 (unknown)
F2:A4:82:14:D5:59 (unknown)
D1:2A:25:D1:71:46 (unknown)
D1:2A:25:D1:71:46 (unknown)
michael@michael-testenv:~$
```

Figure 10: Changing Matter MAC address

To ensure that the MAC address and device are not wrongly assigned during this test, the respective scan was run for 20 seconds so that all BLE devices were detected before the Matter device was switched on. Therefore, the Matter device can be assigned to the lowest MAC address in each test.

Further tests were carried out with the tool `sdptool`. The sdptool enables further information about the device and its functions to be determined using the MAC address (Krasnyansky, N.D.). The results of this test can be found in the Appendix 2. The test revealed a variety of features and information about the Bluetooth device, but none about the BLE device.

Another approach to determine information and potential vulnerabilities of BLE devices was pursued using the `bettercap` tool. The tool bettercap offers a variety of functions to sniff Wi-Fi and BLE networks (Margaritelli et al., 2021). The Ipad, which acted as a hub in the Matter network, and the Matter device were chosen as the sniffing targets for this test. For this purpose, bettercap was first used to search for BLE devices and then the characteristics available via bettercap, services and information about the devices were determined using the 'ble-enum [MAC]' command. Figure 11 shows the results of the BLE sniffing from the iPad.

Figure 11: iPad sniffing with bettercap

The table below in Figure 11 lists the respective handles, which correspond to the functions of the device with Bluetooth, the characteristics and the access authorisations, as well as further information under the Data column. By doing this, some information related to permissions and possible insufficient settings and thus vulnerabilities could be determined. The results of testing the Matter device with bettercap are shown in Figure 12.

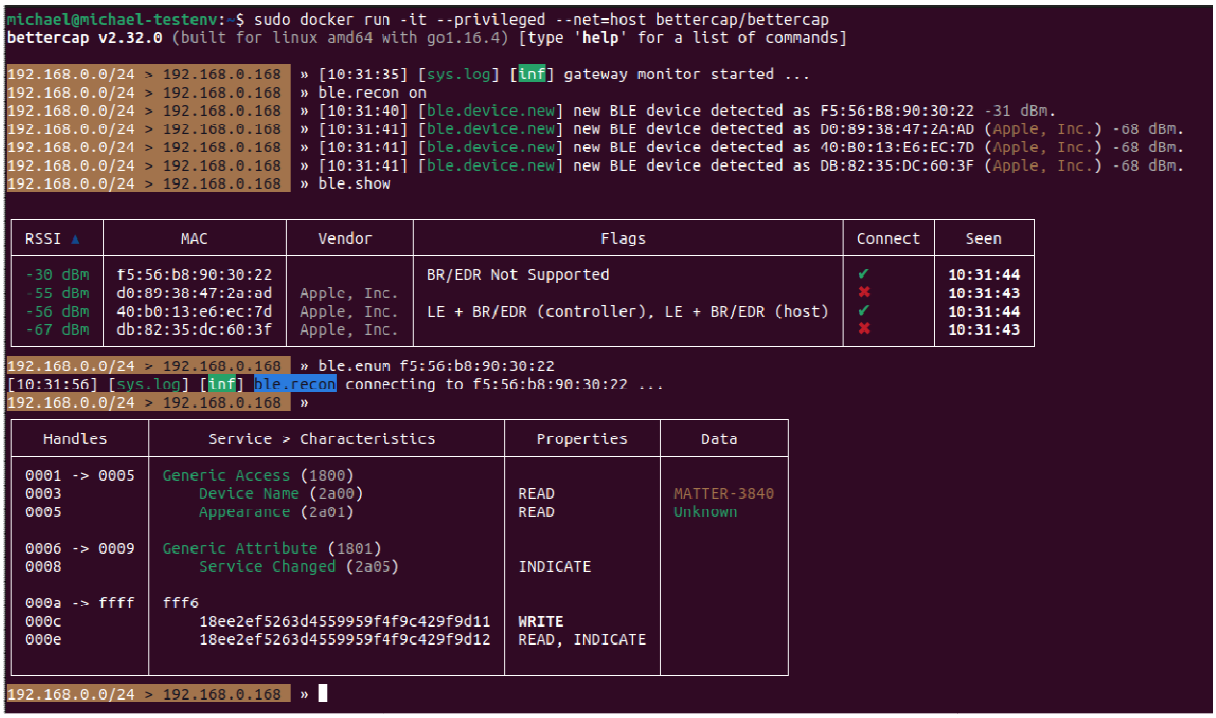


Figure 12: Matter device sniffing with bettercap

While it can be seen that the handles 000c and 000e are encrypted, only the name of the Matter device 'MATTER-3840' could be determined by the handle 0003 by reading the Bluetooth characteristics. The number in the device name is the discriminator of the device, which was already assigned to the device during the flash process and is required for commissioning in a network (CSA, 2022c).

Finally, as part of the Bluetooth sniffing experiments, an attempt was made to read the communication between two devices during the pairing process. For this purpose, the Wireshark tool was used, which enables the capturing of different communication standards (Combs, N.D.). A suitable device capable of capturing BLE packets was required so that the sniffing of the Bluetooth communication could be carried out. As part of these tests, the Nordic nRF52840 dongle was used (Nordic, 2022). The process of commissioning BLE devices was chosen because Matter devices automatically set off the BLE functions after commissioning the device in a network. Furthermore, sensitive data such as the encryption and the password of the Wi-Fi network are sent during this process, so that the commissioning represents a vulnerable process. In order to minimise the probability of incorrect measurements, this test was carried out 10 times for the comparison device and the Matter device.

The commissioning of an Apple Watch was examined as a comparative test. A section of intercepted packets during commissioning can be seen in Figure 13, the complete protocol in Appendix 3.

No.	Time	Source	PHY	Protocol	Length	Delta time (µs end to start)	SN	NESN	More Data	Event counter	Info
3277	67.856	42:06:94:cb:69:4e	LE 1M	LE LL	37	515µs				0	ADV_IND
3278	67.857	52:4a:7a:e3:62:87	LE 1M	LE LL	34	151µs				0	CONNECT_IND
3279	67.878	Master_0x50656d28	LE 1M	LE LL	6	21495µs	0	0	False	0	Control Opcode: LL_VERSION_IND
3280	67.879	Slave_0x50656d28	LE 1M	LE LL	0	149µs	0	1	True	0	Empty PDU
3281	67.879	Master_0x50656d28	LE 1M	LE LL	0	151µs	1	1	False	0	Empty PDU
3282	67.908	Master_0x50656d28	LE 1M	LE LL	0	29412µs	1	1	False	1	Empty PDU
3283	67.909	Slave_0x50656d28	LE 1M	LE LL	6	149µs	1	0	True	1	Control Opcode: LL_VERSION_IND
3284	67.909	Master_0x50656d28	LE 1M	LE LL	0	151µs	0	0	False	1	Empty PDU
3285	67.909	Slave_0x50656d28	LE 1M	LE LL	9	149µs	0	1	True	1	Control Opcode: LL_SLAVE_FEATURE_REQ
3286	67.910	Master_0x50656d28	LE 1M	LE LL	0	151µs	1	1	True	1	Empty PDU
3287	67.910	Slave_0x50656d28	LE 1M	LE LL	0	149µs	1	0	False	1	Empty PDU
3288	67.910	Master_0x50656d28	LE 1M	LE LL	6	151µs	0	0	False	1	Control Opcode: Unknown
3289	67.910	Slave_0x50656d28	LE 1M	LE LL	0	149µs	0	1	False	1	Empty PDU
3290	67.938	Master_0x50656d28	LE 1M	LE LL	9	28143µs	1	1	False	2	Control Opcode: LL_FEATURE_RSP
3291	67.939	Slave_0x50656d28	LE 1M	LE LL	2	150µs	1	0	True	2	Control Opcode: LL_UNKNOWN_RSP
3292	67.939	Master_0x50656d28	LE 1M	LE LL	0	150µs	0	0	False	2	Empty PDU
3293	67.968	Master_0x50656d28	LE 1M	LE LL	0	29373µs	0	0	True	3	Empty PDU
3294	67.969	Slave_0x50656d28	LE 1M	LE LL	0	150µs	0	1	False	3	Empty PDU
3295	67.969	Master_0x50656d28	LE 1M	LE LL	6	150µs	1	1	False	3	Control Opcode: Unknown
3296	67.969	Slave_0x50656d28	LE 1M	LE LL	0	150µs	1	0	False	3	Empty PDU
3297	67.998	Master_0x50656d28	LE 1M	LE LL	0	29183µs	0	0	False	4	Empty PDU
3298	67.999	Slave_0x50656d28	LE 1M	LE LL	6	150µs	0	1	True	4	Control Opcode: Unknown
3299	67.999	Master_0x50656d28	LE 1M	LE LL	0	150µs	1	1	False	4	Empty PDU
3300	67.999	Slave_0x50656d28	LE 1M	LE LL	0	150µs	1	0	False	4	Empty PDU
3301	68.028	Master_0x50656d28	LE 1M	LE LL	3	29182µs	0	0	False	5	Control Opcode: LL_PHY_REQ
3302	68.029	Slave_0x50656d28	LE 1M	LE LL	0	150µs	0	1	False	5	Empty PDU
3303	68.058	Master_0x50656d28	LE 1M	LE LL	0	29667µs	1	1	False	6	Empty PDU
3304	68.059	Slave_0x50656d28	LE 1M	LE LL	3	150µs	1	0	True	6	Control Opcode: LL_PHY_RSP

Figure 13: Commissioning Apple Watch package sniffing

The test shows that the first communication could be recorded. However, it had to be determined that all captured packets were encrypted and the exchange of keys could not be captured. After the first information had been exchanged, eavesdropping was no longer possible and the further course of commissioning was secret.

For the test of sniffing of the commissioning process of the Matter device, an ESP32 controller freshly flashed with the lighting app was integrated into a Matter network with an iPad as a hub. For this purpose, the Matter device was searched for on the iPad and commissioning process was initialised. The complete protocol of the collected packages of a commissioning can be found in Appendix 4. As in the comparison test, the communication could be monitored via Wireshark. However, compared to the previous tests, it was possible in some scans to listen to the complete communication of the commissioning up to the end. A sample package from this process is shown in Figure 14.

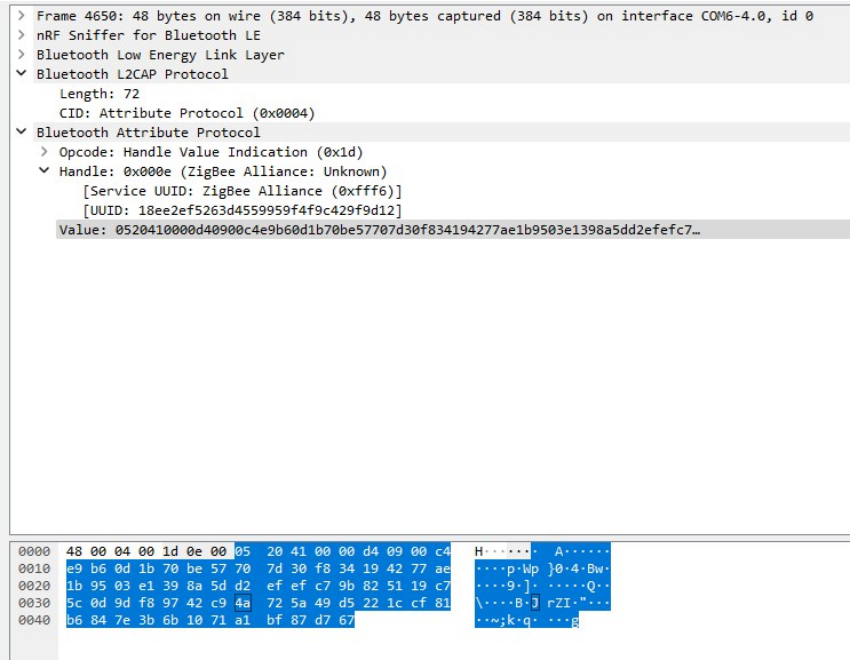


Figure 14: Sniffed Matter commissioning package

This packet shows that various information such as the UUID can be determined by capturing the BLE packets. However, the actual packet content was encrypted as in the comparison test and the initial exchange of the key could not be identified. After the Matter device was successfully integrated into the network, all communication via BLE was stopped by the Matter device.

5.2 Hacking attacks against Wi-Fi

Wi-Fi is the most widely used standard for realising home networks. The standard has security mechanisms such as WPA3, which are used for encryption. In addition to the assumption that WPA3 no longer has to be classified as completely secure, other methods can be found to exploit vulnerabilities in the standard and carry out attacks against Wi-Fi networks (Baray & Ojha, 2021). Two important approaches for attacks against Wi-Fi networks are de-authentication and replay attacks, which were carried out on Matter networks as part of the project to investigate Matter's resilience to these types of attacks.

5.2.1 De-authentication attack

A de-authentication attack aims to interrupt a client's connection to an AP and therefore falls into the category of a denial of service attack. De-authentication frames are packets based on the IEEE 802.11 standard, which are sent to terminate an existing connection (IEEE Standards Association, 2021). After the target has received these packets, all further packets from the affected devices are rejected until re-establishing of the connection occurs via a handshake.

In a de-authentication attack, the attacker pretends to be either the AP or the target device. A schematic representation can be seen in Figure 15.

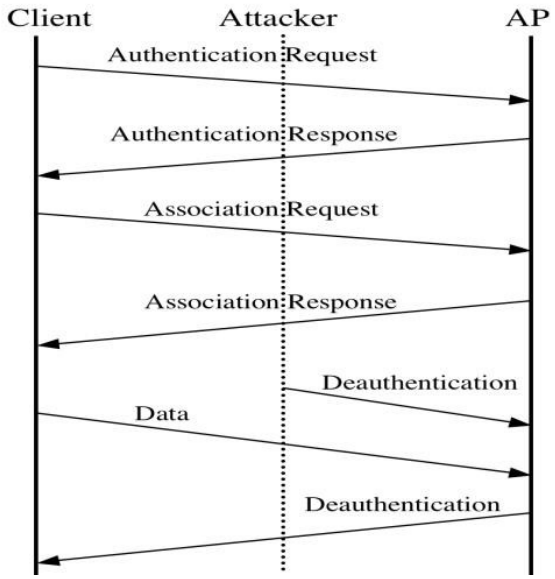


Figure 15: De-authentication attack schematic (Noman, et al., 2015)

The attacker sends spoofed de-authentication packets to the target device or AP that appear to be trying to disconnect. Once the target device or AP receives the spoofed de-authentication packets, they interpret them as legitimate disconnect requests (Kristiyanto & Ernastuti, 2020). As a result of the attack, communication within the network is disrupted and the client no longer has access to the network. The target device must re-authenticate and reconnect to the network to re-establish the communication, but this can be prevented by the attacker by repeated de-authentication frames.

In order to test and compare the resilience of Matter devices to de-authentication attacks, attacks were carried out on the AP and the device of the Matter network. The comparative study was carried out using a test network consisting of an AP provided by an Android smartphone (HUAWEI P30) and a computer, which acted as a device. A test was also

executed in which the same computer was connected to the Matter network router and this AP was attacked. The attack was carried out by the WiFi Deauther Mini V3 development board. This is based on the ESP8266 microcontroller, which is able to scan for Wi-Fi devices and APs and then carry out targeted attacks on the devices found (Kristiyanto & Ernastuti, 2020).

5.2.1.1 De-authentication attack execution and results

First, the de-authentication attacks were carried out on the test network of the smartphone and the computer. The attack on the computer can be seen in Figure 16.

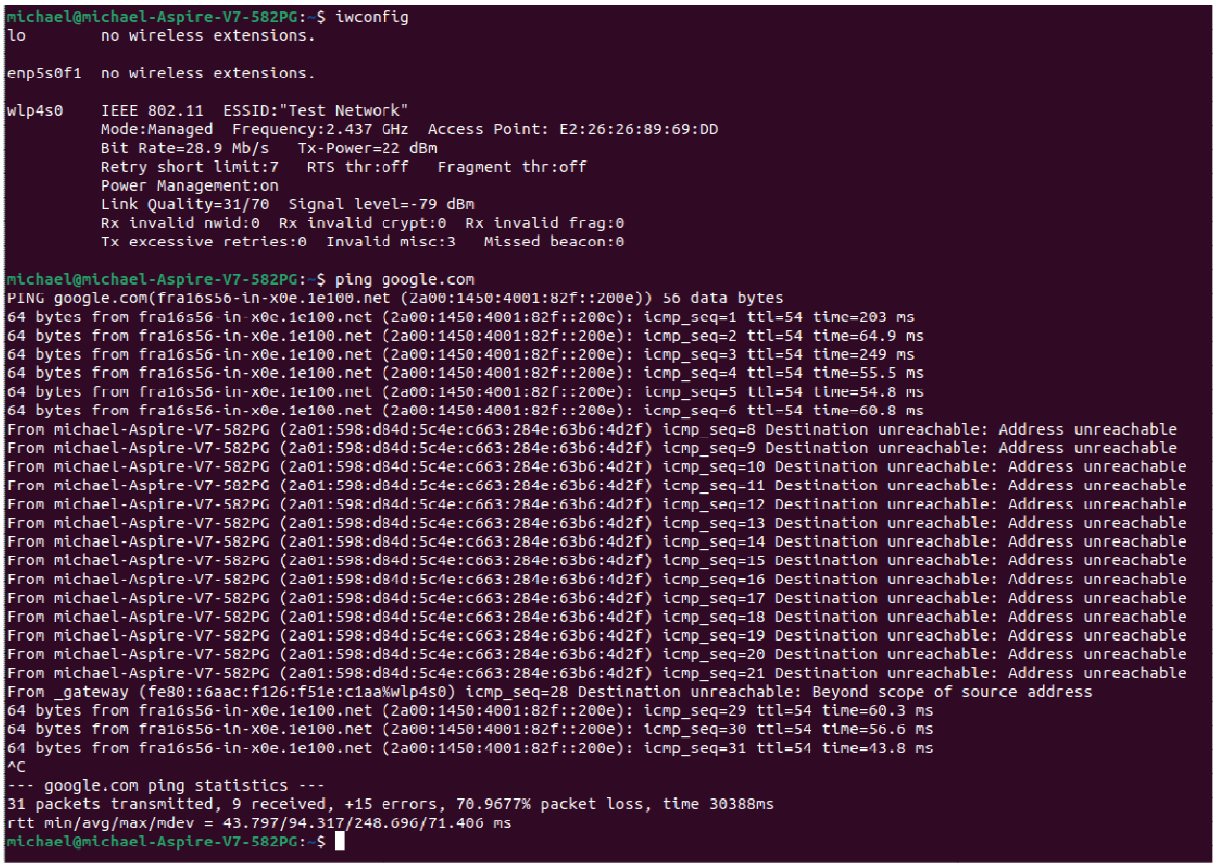


Figure 16: De-authentication of test network, computer attacked

Based on the observations, it can be stated that as soon as the de-authentication attack took place, the Wi-Fi communication with the AP was disrupted. The computer was still connected to the AP, but the ping request was reported as unreachable during the attack. After the end of the attack, the connection was restored, which can be confirmed by the response to the ping request.

The attack on the AP connected to the computer produced similar test results. The test can be seen in Appendix 5. A difference to the previous test with the computer as the target of the attack was that the connection between the computer and the AP was lost during the attack on the AP. Only after the attack ended could the computer find the Wi-Fi network again and establish a new connection. Both of the previous tests were also carried out with the AP via which the Matter network also communicates. The same computer was used here as for the network test. The results of the test can be seen in Appendix 6 and 7.

Based on these tests, it could be determined that an attack on the AP as well as the computer does not lead to any impairment of communication. The same attacks were also carried out against the Matter network. The test result against the AP of the Matter network can be seen in Appendix 8 and against the Matter device in Appendix 9. The same result was observed in both tests. The attack against the AP as well as against the device leads to a termination of communication. This can be seen from the response 'app-devicecallbacks: Lost IPv4 (IPv6) connectivity...'. During the attacks, the device repeatedly tries to reconnect, but without success. A new connection could only be restored after the attacks had ended.

5.2.2 Replay attack

A replay attack is a cryptanalytic form of attack on the authenticity of data in a network. Here, an attacker sends previously recorded data packets to impersonate a legitimate identity and execute a command. Thus, the replay attack falls into the spectrum of man-in-the-middle attacks. Since the successful execution of a replay attack can result in unauthorised commands being resent as often as required, this type of attack poses a serious risk, as it can have a significant impact on the function of devices in a network.

5.2.2.1 Replay attack execution and results

A Python script was created to test the data integrity of Matter devices using a replay attack. The scapy tool was used for this, with which recorded packets can be read in, individual components manipulated and the changed packets finally sent again (Scapy, N.D.). Wireshark was used to intercept the originally sent packets. In order to confirm the functionality of the created Python script, a test network was created by creating a master-client network between

two Ubuntu 22.04 TLS computers and the communication via the freely chosen port 9999 was recorded. Figure 17 shows the Python script used.

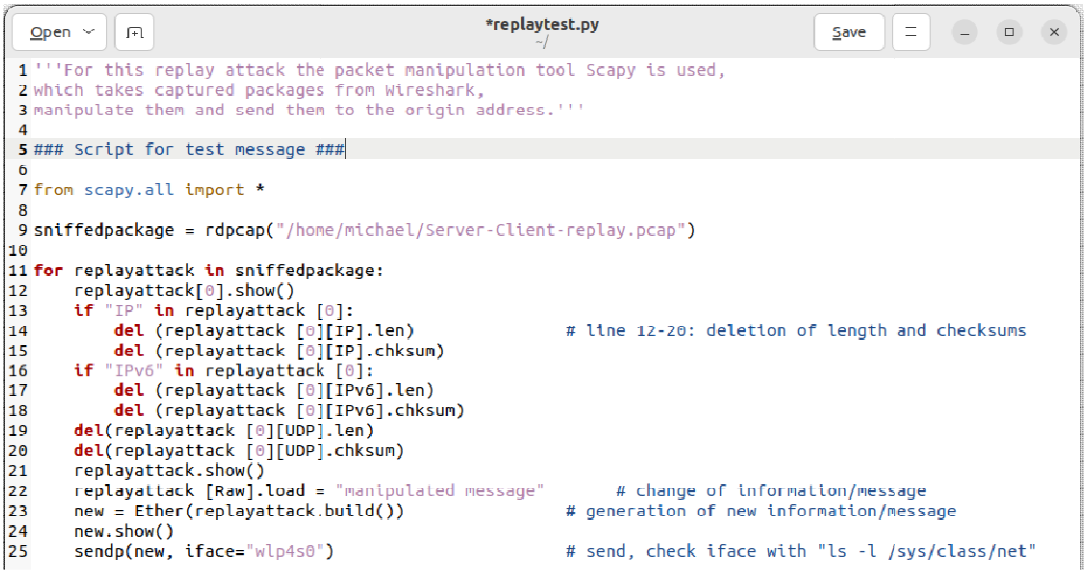


Figure 17: Replay attack python script for comparison test

In the created script, previously collected packets are read using a pcap file, which can be seen in line 10. Then, in lines 12 to 20, the length specifications and checksums are deleted at the IP and UDP level. In line 22, the information content is changed, in this case the message, and then in line 23 the deleted information is regenerated. Finally, in line 25, the manipulated packets are sent via a selected network connection.

Figure 18 shows the messages sent on the client side and Figure 19 shows the packets captured using Wireshark on the server side.

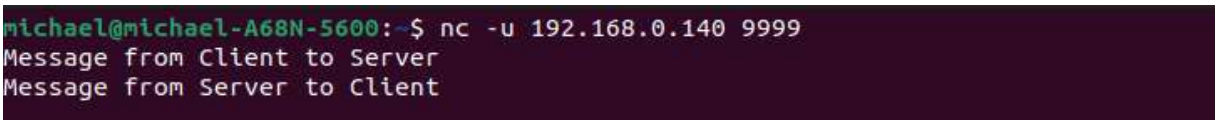


Figure 18: Client-Server terminal communication

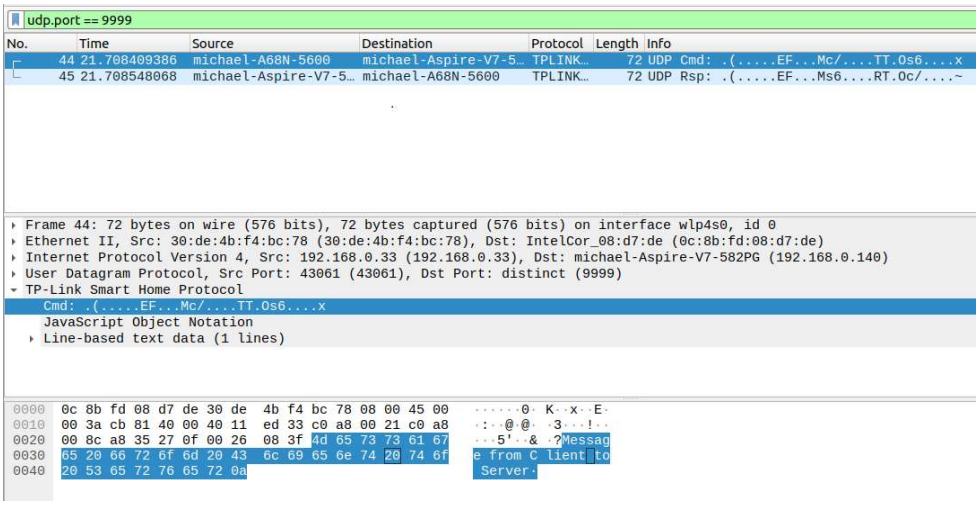


Figure 19: Captured Client-Server communication via Wireshark

The packets recorded by Wireshark can be used to find out some information about the data exchange between the devices involved. In this way, the names and IP addresses of the sender and recipient can be seen. Furthermore, the previously selected port, via which the communication takes place, and finally also the content, in this case the message that was transmitted by the packet, could be displayed. The UDP packet from server to client was then saved in isolation and the Python script executed, see Appendix 10. After the replay attack was carried out, the manipulated content of the message 'manipulated message' was displayed on the client side, as can be seen in Figure 20.

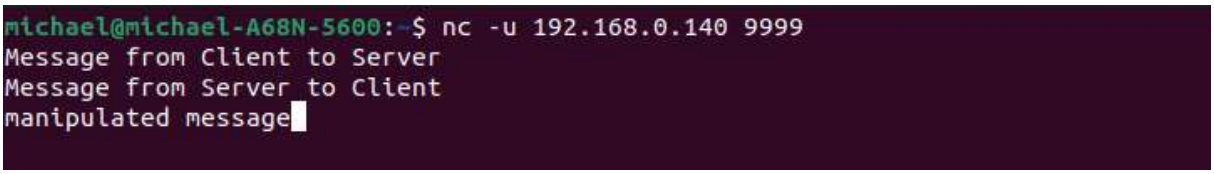


Figure 20: Client-Server replay attack result

The same procedure was now used to test Matter devices for replay attacks. For this purpose, an ESP32 controller with the Matter lighting app application was integrated into a network with a computer as a hub. With the Matter controller implementation chip-tool it is possible to integrate Matter devices into a network by using a computer as a hub to perform tests on the Matter device (Kajor et al., 2023). After the Matter device was integrated into the network, the LED of the Matter device was switched on via chip-tool. The packets sent were now recorded again using Wireshark, see Figure 21.

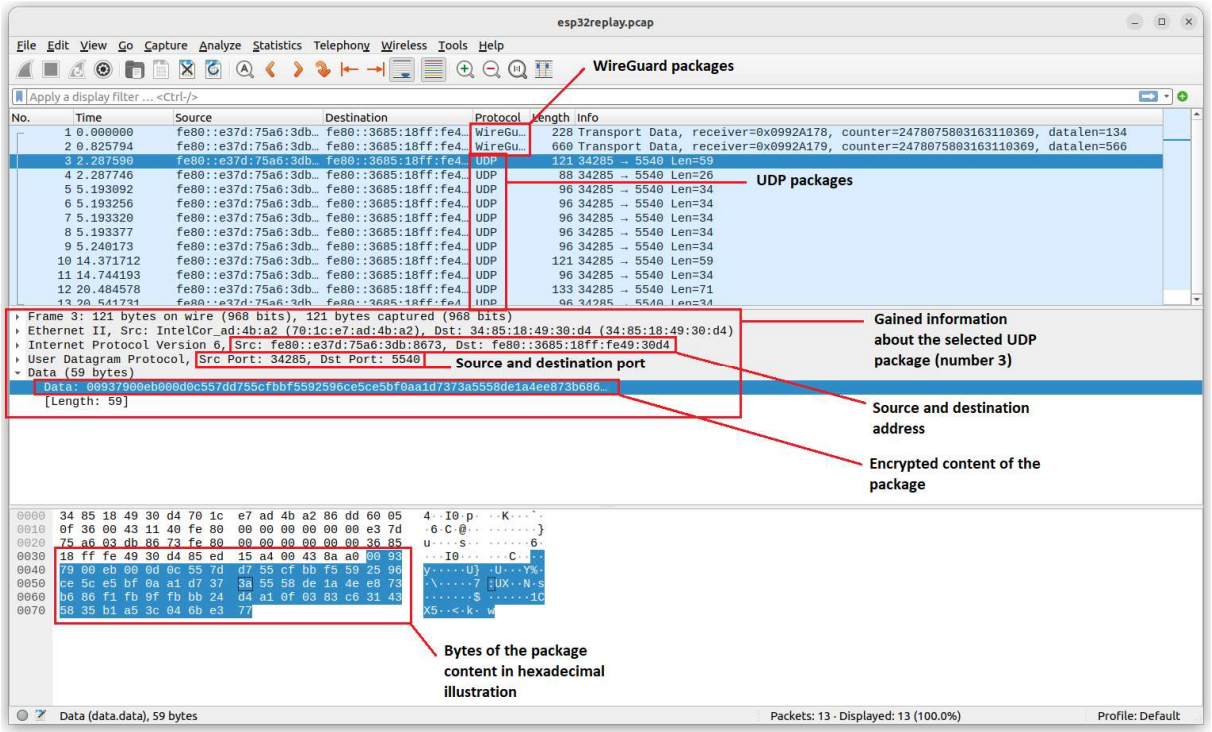


Figure 21: Captured Matter communication via Wireshark

The packets show that initially WireGuard protocol packets are sent and the subsequent communication takes place via UDP packets. It should be noted that the content of the WireGuard packets is specified as 'Encrypted Packet', while the content of the UDP packets is readable but encrypted. After the packets sent during the switch-on process of the Matter device's LED were successfully intercepted, the LED was switched off again and it was tried to repeat the switch-on process using a replay attack. For this purpose, the previously used Python script was used in a slightly different form, which can be seen in Figure 22.

Open Save replayatt_matter.py ~/

```
'''For this replay attack the packet manipulation tool Scapy is used,
which takes captured packages from Wireshark,
manipulate them and send them to the origin address.'''


# Script for matter test #

from scapy.all import *

sniffedpackage = rdpcap("/home/michael/Desktop/esp32replay.pcap")

for replayattack in sniffedpackage:
    replayattack[0].show()
    if "IP" in replayattack [0]:
        del (replayattack [0][IP].len)
        del (replayattack [0][IP].chksum)
    if "IPv6" in replayattack [0]:
        del (replayattack [0][IPv6].len)
        del (replayattack [0][IPv6].chksum)
    del(replayattack [0][UDP].len)
    del(replayattack [0][UDP].chksum)
    replayattack.show()
    new = Ether(replayattack[0].build())
    new.show()
    sendp(new, iface="wlp4s0")                    # send, check iface with "ls -l /sys/class/net"
```

Figure 22: Matter replay attack python script

After executing the replay attack, it was determined that the Matter device received the packets, which can be seen in Figure 23.

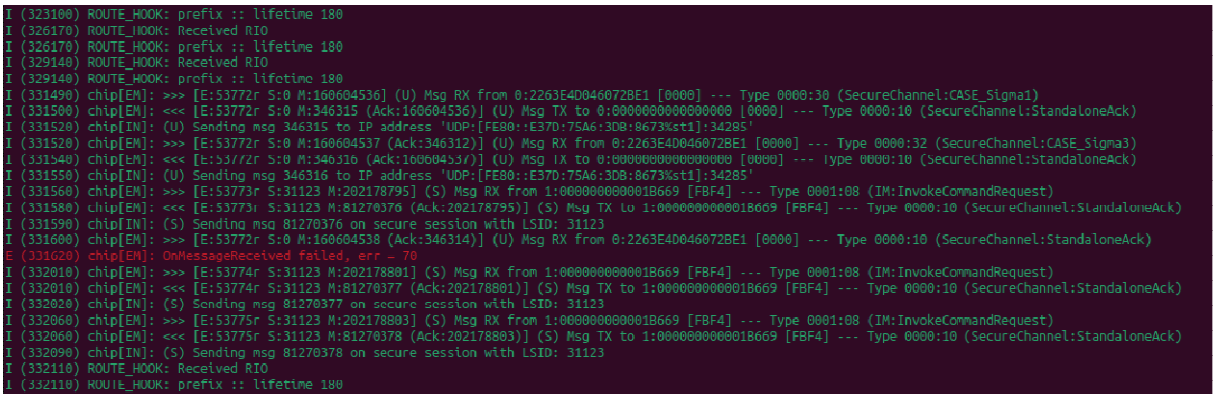


Figure 23: Matter replay attack execution result

Despite receiving the packages, however, they were rejected and the LED could not be switched on as a result. To verify this observation, this test was repeated 10 times, each time giving the same result.

5.3 Further results

When carrying out the tests, some observations could be made which could not be explicitly counted among the experiments, but nevertheless have an added value and are therefore noted at this point.

It was found that the choice of hub device, which is responsible for controlling the Matter devices in a network, has an impact on the usability of non-certified Matter devices. Two hubs were used to conduct the tests. The first hub was a third generation iPad, the second hub device was a second generation Google Nest Hub. Both hub devices recognised the self-flashed microcontroller as a non-certified device. While the iPad warned that the device being paired was an uncertified device and it was possible to decide to take the risk, the Google Nest Hub device aborted the commissioning of the Matter device. Only the notification was displayed that the device to be paired was a non-certified device. It was not possible to accept the risk, so the microcontrollers flashed for the experiments could not be operated with the Google Nest Hub.

It was also determined during the experiments that the integration of the flashed devices into the Matter network was not always successful. In about 20% of the attempts to connect the Matter microcontroller to the iPad as a hub device, commissioning was carried out and

feedback was given that the process was successfully completed. However, it was not possible to operate the controller via the hub. The Hub device could not find the Matter device, although the commissioning was classified as successful immediately before. By monitoring the Matter device, it could also be determined that the device has access to the Wi-Fi network, so that a missing connection to the network is considered unlikely. Furthermore, the commissioning was completed, so that a new attempt to integrate the device into the network was not possible because BLE was switched off. Since the hub device could not communicate with the Matter device, it was also not possible to decouple the device from the network. The only solution found to pair the controller with the hub again was to delete the Matter device from the hub and flash the microcontroller again. A conclusive explanation as to why in some cases the connection between the Matter device and the hub did not work could not be found.

6. Discussion

Based on the tests carried out, some conclusions can be drawn regarding the security of the Matter communication standard, which are reflected in the following.

6.1 Bluetooth sniffing

Tests based on the Bluetooth standard determined that Matter devices do not have static MAC addresses. After switching the Matter device on again, a randomised MAC address was assigned to the device. While the implementation of randomised MAC addresses is stated in the Matter specifications, it is not clear here that this design of the MAC addresses is an explicit security feature (CSA, 2022b). However, it can be assumed that this feature was used for security reasons. The randomisation of the MAC address strengthens some security aspects that can be considered problematic under Bluetooth. A random MAC address makes it difficult for an attacker to commission to a Matter device before the legitimate user. In the case of a static address, this could be carried out in a targeted and automated manner, making it impossible for the legitimate user to integrate the device into the network (Kalantar et al., 2018). Furthermore, the investigation using bettercap did not lead to any recognisable vulnerabilities. By reading the handles, only the name of the device and the discriminator was found out.

The final BLE test of sniffing the exchanged data packets during the commissioning process via Wireshark and the nRF52840 dongle led to inconsistent results. In some implementations of the Matter device's sniffing attack, the complete process of commissioning could be recorded, but in most cases the eavesdropping attack stopped before commissioning was complete. Furthermore, it was not possible to find the exchange of the encryption in any of the tests carried out, so that it was not possible to determine the content of the exchanged packets. Thus, the greatest threat, determining the access data to the Wi-Fi network, could not be confirmed during the tests. However, the possibility of sniffing the commissioning process via Bluetooth does not exclude this threat.

Another interesting observation that could be made during the commissioning of Matter devices is the different security functions that emanate from the hub device. While the iPad as a hub allows the integration of devices not certified by Matter as a risk, the non-certified Matter device was rejected by the Google Nest Hub. This shows that the device developers

are given some freedom with regard to security aspects. Furthermore, this observation shows that in some cases a trade-off between security and usability has to be made. In the case of the iPad, this decision was made in favour of usability, allowing potentially malicious devices to infect the network. The Google Nest Hub, on the other hand, relies on security, which, however, prevents the creation and the use of non-certified Matter devices, thus limiting interoperability.

These two aspects contradict each other to a certain extent by the claims that Matter makes of itself, since on the one hand interoperability has been stated as a central goal of Matter and on the other hand CSA claims that 'Customers buying Matter devices will not have to think about security: it is just there' (CSA, 2022a). These two approaches of prioritising Matter functions by the manufacturers mean that Matter vulnerabilities can be device-specific in the future, which means that, contrary to CSA's claims, users have to be aware of the security of Matter.

6.2 De-authentication attack

A summary of the test results of the de-authentication attacks carried out is listed in Table 2.

Table 2: Compilation of de-authentication attacks results

Network	Attacked target	Deauthentication attack
Computer - Test AP	Device	successful
Computer - Test AP	AP	successful
Matter device - Matter AP	Device	successful
Matter device - Matter AP	AP	successful
Computer - Matter AP	Device	unsuccessful
Computer - Matter AP	AP	unsuccessful

During the tests, it was found that neither the test network, consisting of a smartphone as an AP, nor the Matter network is protected against de-authentication attacks. However, the execution of a de-authentication attack on the computer used in the test network, connected to the AP used for the Matter network, was unsuccessful.

Furthermore, it was determined that when a device was attacked, it lost the connection to the network, but not other devices that were connected to the AP. In the event of an attack on the

AP, all or just some devices in the network were affected, depending on the AP. This finding suggests that the properties of the AP or the device are not the only prerequisites for preventing de-authentication attacks. Rather, it is the compatibility of both participating network components that determines the vulnerability with regard to de-authentication attacks. A search for an explanation of the results obtained in this test leads to the assumption that the IEEE 802.11w supplement to the Wi-Fi standard is the cause of the observed results (IEEE 802 LAN/MAN Standards Committee, 2009).

The IEEE 802.11w standard ensures that management and control information transmitted in an 802.11 WLAN is encrypted (Qureshi & Asghar, 2023). This is intended to prevent attackers without a valid key from disrupting communication in the WLAN or from being able to penetrate the network. Encrypted management information, known as Protected Management Frames (PMF), ensures the integrity of network management traffic and increases the WLAN's resilience to attacks. However, to use the security function, both the AP and the WLAN client must support PMF.

In order to encrypt the management frames, it is also necessary for the WLAN environment to support WPA2 (Chen & Punya, 2020). However, it should be noted that only a few Wi-Fi devices under WPA2 have integrated the IEEE 802.11w supplement (Lounis et al., 2021). For the latest WPA3 standard, PMFs are an integral part. The monitoring of an integrated Matter ESP32-S3 controller has shown that the security standard WPA2 is used in the tested Matter network, which can be seen in Figure 24.

```
I (1138) wifi:connected with Vodafone-0A14, aid = 22, channel 11, BW20, bssid = 1c:9e:cc:3a:0a:18
I (1158) chip[DMG]: DefaultAclStorage: 1 entries loaded
I (1158) wifi:security: WPA2-PSK, phy: bgn, rssi: -26
I (1178) wifi:pm start, type: 1
```

Figure 24: WPA2 encryption of the Matter device

However, an examination of the Matter specifications showed that Matter does support WPA3 (CSA, 2022c). Research into the security standards of the ESP32-S3 controller used also revealed that the device supports WPA3 as a security feature (Espressif Systems, 2023). It therefore had to be assumed that the router used for the Matter network only has the WPA2 security standard, which could be confirmed by looking at the router settings.

Finally, it was found that Matter is protected against de-authentication attacks within the framework of a WPA3 environment, but this requires that all devices in the network are WPA3 compatible. In the test scenario carried out, however, the AP was only compatible with WPA2, so the security standard was downgraded to WPA2. Under this security standard, the

Matter device was not protected against de-authentication attacks, since the IEEE 802.11w supplement to the Wi-Fi communication standard was not implemented. A search in the Matter specifications did not contain any information on IEEE 802.11w (CSA, 2022c). It can therefore be concluded that under WPA2 Matter devices are not adequately protected against de-authentication attacks. This increases the potential threat of downgrade attacks in which older WPA security standards are specifically exploited (Lamers et al., 2021).

6.3 Replay attack

As part of the intended test of a replay attack on a Matter device, a Python script was created with the scapy tool, which can resend data packets intercepted via Wireshark. In order to be able to confirm the functionality of the script, the message exchange between a client-server structure of two Ubuntu 22.04 TLS computers was intercepted, the content of a UDP packet was manipulated and sent again.

However, the execution of replay attacks on Matter devices with the lighting-app application showed that no vulnerabilities of Matter with regard to replay attacks could be detected in the scenario used. Based on the monitoring of a Matter controller during a replay attack, which can be seen in Figure 23 in Chapter 5.2.2.1, it can be confirmed that the packets resent by the Python script were received by the Matter device. In addition to the observation that the LED was not switched on by these packets, the error message 'OnMessageReceived failed, err = 70' could also be determined. The Matter specification does not provide any information regarding this error message (CSA, 2022c). However, it was possible to find out, that the error message 70 stands for "CHIP_ERROR_UNSOLICITED_MESSAGE_NO_ORIGINATOR" (Shripad621git, 2023). This error message occurs when a message was detected that was sent from an unauthorised source or does not conform to session integrity. Since the replay attacks were carried out by the same computer from which the packets recorded for the test were sent, it is likely that the message counter recognised the packets that were sent again as invalid. The message counter is used by Matter to ensure packet integrity and is randomly initialised at the beginning of each session and then incremented with each outgoing message (CSA, 2022c). It can therefore be concluded that the replay attack could be warded off as a result of inconsistency of the session integrity, recognised by the message counter.

With regard to the replay attacks carried out, it should be emphasised that all tests were executed with packets that were recorded directly on the sender's computer. As part of the

experiments, it had to be determined that recording the Wi-Fi communication turned out to be difficult and various approaches to reading out the data traffic via Wireshark failed.

On the one hand, an attempt was made to remotely record the data traffic of the network in which the Wi-Fi dongle tp-link TL-WN722N and BrosTrend AC1200, which are supposed to support the monitor mode required for remotely capturing Wi-Fi packets (WikiDevi, 2021; SecWiki, N.D.). However, it was found that the chipset of the TL-WN722N has changed and the chip that is now in use no longer supports monitor mode. With the BrosTrend AC1200 Wi-Fi adapter, a basic recording of the data traffic of packets could be made, but the packets sent from the client-server structure and between the Matter components could not be found. It must be noted here that wireless acquisition is difficult due to various factors such as physical characteristics of the devices and supported operating system drivers, and if successful, the amount of data easily exceeds the capacities of the hardware and software due to the unfiltered data acquisition (Kismet, N.D.).

Attempts to scan the traffic packets of the Matter network via the iPad used as a hub device also failed. An attempt was made to establish a remote virtual interface between an Apple computer and the iPad in order to record the communication via this connection using Wireshark. However, it had to be determined that the available devices (iPad generation 1-3 and MacBook os El Capitain v. 10.11.16) are not compatible with each other or the versions of the iPad are too old to be compatible with Matter. Furthermore, an attempt was made to create an AP for the Matter network with the operating systems Ubuntu 22.04 TLS and OpenWRT 22.03.5. However, the result was that the iPad could not be connected to the Ubuntu 22.04 TLS as an AP and the commissioning of the Matter device with the hub was not successful under OpenWRT. These results offers the realisation that the acquisition of Wi-Fi data packets using Wireshark is made more difficult due to various factors such as hardware, compatibility of operating systems and interoperability between different versions.

6.4 Verification and validation

With regard to Bluetooth sniffing, it can be stated that the experiments were carried out successfully and that comparable results from Matter and test networks were recorded. However, since the test with bettercap with the iPad as a comparison device led to similar results as with the Matter device, these tests could only determine that this method enables possible vulnerabilities to be spied out in insufficiently implemented BLE devices. Choosing

a device with known vulnerabilities would therefore have led to more meaningful results at this point. Nevertheless, it can be stated that no vulnerabilities of the Matter device could be identified in the course of this experiment.

Furthermore, the Bluetooth package capturing of the commissioning process also led to valuable results, which, however, have deficiencies in terms of consistency. In 10 consecutive tests, the complete process could be recorded in 2 cases and only parts of it in 8 cases. An examination of the last collected packets of the respective tests revealed that there was no recognisable regular place for the termination of the sniffing attack. The last recorded write requests each referred to different handles, so the abort appears random. However, incorrect execution of the tests, for example due to the selection of an incorrect MAC address, can be ruled out because, contrary to the inconsistent completion of the tests, the beginning of each recording took place with the exchange of the same packets and these can be found in every test run. Figure 25 shows the initial exchange of packages during the commissioning process.

3147	4525.7…	Master_0x5065451e	LE 1M	LE LL	6	17267µs	0	0	False	0	Control Opcode: LL_VERSION_IND
3148	4525.7…	Slave_0x5065451e	LE 1M	LE LL	9	151µs	0	1	True	0	Control Opcode: LL_SLAVE_FEATURE_REQ
3149	4525.7…	Master_0x5065451e	LE 1M	LE LL	0	150µs	1	1	False	0	Empty PDU
3150	4525.7…	Slave_0x5065451e	LE 1M	LE LL	0	151µs	1	0	False	0	Empty PDU
3151	4525.7…	Master_0x5065451e	LE 1M	LE LL	9	21609µs	0	0	False	1	Control Opcode: LL_FEATURE_RSP
3152	4525.7…	Slave_0x5065451e	LE 1M	LE LL	6	150µs	0	1	True	1	Control Opcode: LL_VERSION_IND
3153	4525.7…	Master_0x5065451e	LE 1M	LE LL	0	151µs	1	1	False	1	Empty PDU
3154	4525.7…	Slave_0x5065451e	LE 1M	LE LL	0	150µs	1	0	False	1	Empty PDU
3155	4525.8…	Master_0x5065451e	LE 1M	LE LL	3	21609µs	0	0	False	2	Control Opcode: LL_PHY_REQ
3156	4525.8…	Slave_0x5065451e	LE 1M	LE LL	0	151µs	0	1	False	2	Empty PDU
3157	4525.8…	Master_0x5065451e	LE 1M	LE LL	0	22166µs	1	1	False	3	Empty PDU
3158	4525.8…	Slave_0x5065451e	LE 1M	LE LL	3	151µs	1	0	True	3	Control Opcode: LL_PHY_RSP
3159	4525.8…	Master_0x5065451e	LE 1M	LE LL	0	150µs	0	0	False	3	Empty PDU
3160	4525.8…	Slave_0x5065451e	LE 1M	LE LL	0	151µs	0	1	False	3	Empty PDU
3161	4525.8…	Master_0x5065451e	LE 1M	LE LL	5	21704µs	1	1	False	4	Control Opcode: LL_PHY_UPDATE_IND

Figure 25: Sniffed initial Bluetooth packages

These results suggests that the different results of the sniffing attacks cannot be explained by channel hopping and the associated randomly recorded sections of the process, since otherwise the first detected packets would not have been recorded in all test runs. However, it can be assumed that the nRF52840 dongle has a significant impact on the test and thus the results. The sniffing device used in the tests is a Bluetooth sniffing dongle, which is located at the lower end of the price segment. Better and therefore more expensive devices have a better quality of packet recording, so it can be assumed that a better sniffing device could have led to more consistent results (Scheible, 2020). It therefore had to be determined that the capturing of Bluetooth packets is not as consistent as assumed.

With regard to de-authentication attacks, it can be stated that verification of the executions can be confirmed. Since each of the test scenarios was performed 10 times and the results were the same according to the devices involved, it can be assumed that the experiments could be carried out consistently and in a target-oriented manner. Due to the reproducibility of the results, sources of interference that lead to the test results are considered unlikely.

A verification of the experiments of the replay attack can also be confirmed. Since the simulation of a replay attack could be carried out successfully, it can be concluded that the created Python script is able to carry out a replay attack. Since these experiments led to the same, consistent results when repeated 10 times, it can be assumed that the possible vulnerability to be tested was successfully investigated and the test design was created appropriately.

A final validation of the results can be carried out with regard to the respective experiments as well as in the context of the overall project question. The results in relation to Bluetooth suggest that Matter has no vulnerabilities. However, it should be noted that this assessment can only be made on the basis of the test results obtained. It is not possible to rule out threats relating to Matter's Bluetooth components based on the experiments. The conclusion must therefore be drawn that a sufficient assessment with regard to the research question regarding Bluetooth cannot be made.

In contrast to this, a clear validation can be carried out in the context of the de-authentication attack. The results indicate that Matter has identified vulnerabilities in the Wi-Fi component relative to older WPA security protocols supported by Matter. It therefore follows that in this context Matter is not able to fix all security problems of Wi-Fi. The test of replay attacks also leads to a clear finding. It can be seen that Matter was actively mitigating threats of replay attacks.

Table 3: Summary of the test results

Hacking experiment	Outcome
Bluetooth sniffing	No vulnerabilities found.
De-authentication attack	Attack was under WPA2 successful. Matter does not support 802.11w.
Replay attack	Replay attack was not successful on Matter. Attack was prevented by the Message Counter.

It can thus be summarised that, with regard to some aspects, Matter can contribute to a more secure smart home network, but not all vulnerabilities have been sufficiently taken into account. In view of the research question, it can therefore be finally assessed that Matter is not able to solve all security problems of the communication standards used under Matter. Matter thus does not overcome the security problems of implemented communication standards.

6.5 Lessons learned

A variety of devices and tools were used within the project to investigate security aspects. In this way, first experiences with the handling of microcontrollers could be made and learned how they can be built, flashed and utilised as part of a development framework. Furthermore, the in-depth handling of various operating systems such as Ubuntu 22.04 TLS, OpenWRT and macOS was learned, which were only used superficially in the past. Interesting in this context was the experience that the interoperability of different macOS and iOS versions can pose a much bigger problem than initially assumed. The question arises to what extent the lack of interoperability with older devices can be justified with security aspects and what significance the economic interests of the companies have behind this decision.

Regarding Matter, it became clear that the large promises regarding the security of the standard could not be confirmed. No particularly new and outstanding security functions are invented, so it is questionable whether Matter can rule out all risks for smart home networks for users and society. Companies should be aware of this problem and take care about the security of their products independently.

A particularly large increase in knowledge can be found in the context of communication standards, since a theoretical analysis of various standards took place as part of the project and the experiments, but practical tests were also carried out on the Wi-Fi and Bluetooth standards. Through these tests, a reflected understanding of possible threats from attacks could be developed and the vulnerabilities of the corresponding standards were clarified. Thus, the theoretical knowledge about threats based on the Bluetooth standard could be transferred into a practical context, so that application-specific skills could be trained. Furthermore the knowledge could be gained how easy it is to capture the packets of the Bluetooth standard compared to Wi-Fi.

In contrast, the implementation of the Wi-Fi tests was accompanied by some challenges, so that solutions had to be found that promoted personal problem-solving skills. These challenges primarily included capturing Wi-Fi packets and interoperability between devices and Wi-Fi AP. It was interesting to note that capturing packets, especially remotely, is far more complicated than originally expected, but further processing of these packets turned out to be easy. The finding led to the realisation that the primary security of a Wi-Fi network is located in the prevention of intrusion by malicious users.

Competence gains in relation to project planning and time management can also be confirmed, since the project that was carried out was confronted with some challenges, which can be attributed to the relatively new communication standard Matter, but were also due to planning that could be improved.

It should be stated that the planned experiments have exceeded the scope of the project. Due to regulations such as the word limit, it had to be realised that the respective experiments could not be analysed and discussed comprehensively enough. Choosing fewer aspects to be examined would have made it possible to evaluate the results more intensively. For future projects, the realisation was gained that narrower and more focused objectives should be pursued.

7. Conclusion

The investigation of the Matter communication standard with regard to security aspects carried out as part of the project shows that Matter is able to cleverly combine the two standards (Wi-Fi and Bluetooth) with one another. The simple use of Bluetooth provides a user-friendly method of commissioning of new devices into a Matter network, while the communication of existing connections occurs exclusively via Wi-Fi. Since Bluetooth is automatically switched off after the commissioning process, the respective strengths of the standards can be applied in a targeted manner.

The sniffing attacks on Wi-Fi and Bluetooth carried out in the test show that this procedure is also necessary, since capturing the packets under Bluetooth was many times easier and more successful than that of Wi-Fi. It can also be confirmed that some considerations have been made with regard to security aspects of Bluetooth, as can be seen, for example, in the randomisation of the MAC address and the encryption of the communication. However, the sniffing attacks carried out via Bluetooth show that it is possible to record the data exchange when Matter devices are commissioned.

Furthermore, it can be confirmed that Matter supports the latest security standards of Wi-Fi, such as WPA3. The data integrity could also not be attacked in the experiments, which prevented a man-in-the-middle attack as part of a replay attack. However, it had to be determined that basic security functions under the older security protocol WPA2 were insufficiently taken into account in the tested version 1.1 of Matter. So it is not apparent that Wi-Fi's 802.11w security feature is built into and supports Matter. It follows that the current version of Matter is susceptible to de-authentication attacks that are easy to carry out, and communication in a Matter network can therefore be significantly impaired by such attacks. This also amplifies the threats regarding downgrading attacks, causing malicious actions in this context can lead to greater damage.

It can therefore finally be stated with regard to the research question that Matter in the current version is not able to overcome all the vulnerabilities of the standards used for Matter. Although a large number of security aspects are taken into account under Matter, not all proven security functions are used. In addition, Matter is largely based on the recommended procedures of the standards used and uses the security features, but does not expand them further, so that significant reinventions of security aspects could not be found within the framework of the project. It should be noted, however, that Matter is in a published version at

the time the project has been carried out, but it is still relatively early in its development cycle. During the period of this project, it could be observed that intensive work continued on the Matter Repository, so that there is hope that the security of the standard will also be significantly further developed and improved in the further development process of Matter. Whether or not Matter will be the communication standard in the IoT Smart Home area, which makes the multitude of standards currently in use redundant, remains to be seen in the future. However, the mitigation of possible vulnerabilities in the standard, as well as those identified in this project, will be a key factor in Matter establishing itself in the market and user acceptance of this standard.

The experiments carried out in this project form an initial basis for assessing the quality of Matter's security. However, some suggestions for further work can be generated in relation to Matter and as a product of this project. In this project, the Thread communication standard, which is also supported by Matter, was not examined for possible security gaps. Possible vulnerabilities with regard to communication through interoperability between Wi-Fi and thread also represent an interesting basis for further research.

Furthermore, the results of the Bluetooth sniffing of this project offer further research potential in relation to the security of the encryption of the data packets and possible threats to decrypt them. In addition, the discovered threat of possible vulnerabilities related to WPA2 and downgrading attacks on Matter devices is also an item that should be investigated in depth.

Finally, only freshly flashed and non-certified Matter devices were used as part of this project. Due to the observation of the different security features of the hub devices, these also offer further research potential, since on the one hand the question can be asked how secure the certificates are in terms of manipulation. On the other hand, investigating the potential threat of reselling hacked certified Matter devices to secondary consumers offers another comprehensive research spectrum that should be investigated.

References

Abomhara, M. & Køien, G. M. (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility* 4: 65-88. Available from: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/6087 [Accessed 09 May 2023].

Adi, P. D. P., Sihombing, V., Siregar, V. M. M., Yanris, G. J., Sianturi, F. A., Purba, W., Tamb, S. P., Simatupang, J., Arifuddin, R. & Prasetya, D. A. (2021) 'A performance evaluation of ZigBee mesh communication on the Internet of Things (IoT)', *3rd East Indonesia Conference on Computer and Information Technology.* Surabaya, Indoneisa, 09-11 April. IEEE. 7-13. Available from: https://ieeexplore.ieee.org/abstract/document/9431875 [Accessed 17 June 2023].

Akestoridis, D. G., Sekar, V. & Tague, P. (2022) 'On the security of Thread networks: Experimentation with OpenThread-enabled devices', *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks.* San Antonio, Texas, 16-19 May. New York: Association for Computing Machinery. 233-244. Available from: https://dl.acm.org/doi/abs/10.1145/3507657.3528544 [Accessed 21 April 2023].

Alhammadi, N. A. M. & Zaboon, K. H. (2022) A Review of IoT Applications, Attacks and Its Recent Defense Methods. *Journal of Global Scientific Research* 7(3): 2128-2134. Available from: https://www.gsjpublications.com/jgsr15920059.pdf [Accessed 25 March 2023].

Alhamry, M. & Elmedany, W. (2022) 'Exploring Wi-Fi WPA2 KRACK vulnerability: A review paper', *International Conference on Data Analytics for Business and Industry*. Sakhir, Bahrain, 25-26 October. IEEE. 766-772. Available from: https://ieeexplore.ieee.org/abstract/document/10041548 [Accessed 02 September 2023].

Ali, B. & Awad, A. I. (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* 18(3): 817. Available from: https://www.mdpi.com/1424-8220/18/3/817 [Accessed 09 May 2023].

Allhoff, F. & Henschke, A. (2018) The internet of things: Foundational ethical issues. *Internet of Things* 1 55-66. Available from: https://www.sciencedirect.com/science/article/pii/S2542660518300532 [Accessed 03 April 2023].

Alobaidy, H. A., Mandeep, J. S., Nordin, R. & Abdullah, N. F. (2020) A review on ZigBee based WSNs: concepts, infrastructure, applications, and challenges. *International Journal of Electronical Engineering & Telecommunications 9*(3): 189-198. Available from: http://www.ijeetc.com/uploadfile/2020/0414/20200414052006525.pdf [Accessed 18 June 2023].

Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W. & Savaglio, C. (2016) 'A mobile multi-technology gateway to enable IoT interoperability', *IEEE first international conference on internet-of-things design and implementation.* Berlin, Germany, 04-08 April.

IEEE. 259-264. Available from: https://ieeexplore.ieee.org/abstract/document/7471371 [Accessed 24 April 2023].

Appel, M. & Guenther, I. S. (2020) *WPA 3-Improvements over WPA 2 or broken again?*. Munich, Char of Network Architectures and Services, Department of Informatics. Available from: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_02.pdf [Accessed 02 May 2023].

Asadullah, M. & Ullah, K. (2017) 'Smart home automation system using Bluetooth technology', *International Conference on Innovations in Electrical Engineering and Computational Technologies.* Karachi, Pakistan, 05-07 April. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/7916544 [Accessed 26 April 2023].

Atmoko, R. A., Riantini, R. & Hasin, M. K. (2017) IoT real time data acquisition using MQTT protocol. *Journal of Physics: Conference Series* 853(1): 012003. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/853/1/012003/pdf [Accessed 19 June 2023].

Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnosopoulos, M., Spathaoulas, G., Giannoutakis, K. M., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E. & Nijdam, N.A. (2019) 'From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes', *International Workshop on Computer Aided Modeling and Design of Communcation Links and Networks*. Limassol, Cyprus, 11-13 September. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/8858493 [Accessed 01 September 2023].

Badman, L. & Parmenter, T. (2020) What is the difference between WLAN and Wi-Fi?. *TechTarget*. Available from: https://www.techtarget.com/searchnetworking/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN [Accessed 19 April 2023].

Baray, E. & Ojha, N. K. (2021) 'WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique', *5th International Conference on Computing Methodologies and Communication.* Erode, India, 08-10 April. IEEE. 23-30. Available from: https://ieeexplore.ieee.org/abstract/document/9418230 [Accessed 19 July 2023].

Bender, M., Kirdan, E., Pahl, M. O. & Carle, G. (2021) ,Open-source mqtt evaluation', *IEEE 18th Annual Consumer Communications & Networking Conference.* Las Vegas, USA, 09-12 January. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/9369499 [Accessed 19 June 2023].

Bernal, A. J. P., Parra, O. J. S. & López, A. A. (2018) Vulnerabilities and Attacks on WiFi Networks. *International Journal of Applied Engineering Research 13*(15): 12052-12054. Available from: http://www.ripublication.com/ijaer18/ijaerv13n15_49.pdf [Accessed 11 May 2023].

Bluetooth SIG (2023) The Bluetooth Low Energy Primer. Available from: https://www.bluetooth.com/wp-content/uploads/2022/05/The-Bluetooth-LE-Primer-V1.1.0.pdf?__hstc=44473531.2faf1062bd3216c20d1374676e323ce9.1681978224809.168197

8224809.1681978224809.1&__hssc=44473531.6.1681978224809&__hsfp=278970564&hsCtaTracking=8e3cb9ce-2e7b-471a-b5cc-2343a4915b6a%7C090f705a-f0df-4f4b-8a54-c8f97c73eb69 [Accessed 20 April 2023].

Bluetooth SIG (N.D.) Bluetooth Wireless Technology. Available from: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ [Accessed 20 April 2023].

Brantly, A. F. (2017) The violence of hacking: state violence and cyberspace. *The Cyber Defense Review* 2(1): 73-92. Available from: https://www.jstor.org/stable/26267402 [Accessed 04 April 2023].

Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E. & Shoaib, M. (2019) 'IoT smart health security threats', *19th International conference on computational science and its applications.* St. Petersburg Russia, 01-04 July. IEEE. 26-31. Available from: https://ieeexplore.ieee.org/abstract/document/8853599 [Accessed 08 May 2023].

Chantzis, F., Stais, I., Calderon, P., Deirmentzoglou, E. & Woods, B. (2021) *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*. No Starch Press. Available from: https://learning.oreilly.com/library/view/practical-iot-hacking/9781098128876/c02.xhtml#h1-500907c02-0002 [Accessed 23 March 2023].

Chen, C. L. & Punya, S. (2020) 'Enhanced wpa2/psk for preventing authentication cracking', *Mobile Wireless Middleware, Operating Systems and Applications: 9th EAI International Conference, MOBILWARE 2020.* Hohhot, China, 11 July. Springer International Publishing. 156-164. Available from: https://link.springer.com/chapter/10.1007/978-3-030-62205-3_15 [Accessed 22 July 2023].

Chen, F., Huo, Y., Zhu, J. & Fan, D. (2020) ,A review on the study on MQTT security challenge', *IEEE International Conference on Smart Cloud.* Washington, USA, 06-08 November. IEEE. 128-133. Available from: https://ieeexplore.ieee.org/abstract/document/9265962 [Accessed 19 June 2023].

Clutterbuck, P. (2010) 'Spyware Security Management via a Public Key Infrastructure for Client-Side Web Communicating Applications', *10th IEEE International Conference on Computer and Information Technology.* Bradford, United Kingdom, 29 June - 01 July. IEEE. 859-864. Available from: https://ieeexplore.ieee.org/abstract/document/5578087 [Accessed 04 May 2023].

Combs, G. (N.D.) About Wireshark. Available from: https://www.wireshark.org/about.html [Accessed 17 July 2023].

CSA (2021) The Future of IoT is Now: Project Connected Home over IP. Available from: https://www.youtube.com/watch?v=Dqy6ASRgWmI [Accessed 05 April 2023].

CSA (2022a) Matter Security and Privacy Fundamentals. Available from: CSA_Matter_Security_WP.docx (csa-iot.org) [Accessed 06 April 2023].

CSA (2022b) Matter Security and Privacy: A Deep Dive with the Experts – Connectivity Standards Alliance. Available from: https://www.youtube.com/watch?v=Q4jhK-IBKuI [Accessed 04 April 2023].

CSA (2022c) Matter Specification Version 1.0. Available from: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf [Accessed 25 April 2023].

CSA (2023) Matter. Available from: https://github.com/project-chip/connectedhomeip#readme [Accessed 06 April 2023].

CSA (N.D.a) The Foundation for Connected Thing. Available from: https://csa-iot.org/all-solutions/matter/ [Accessed 16 March 2023].

CSA (N.D.b) zigbee – The Full-Stack Solution for All Smart Devices. Available from: https://csa-iot.org/all-solutions/zigbee/ [Accessed 19 June 2023].

CSA (N.D.c) Zigbee FAQ. Available from: https://csa-iot.org/all-solutions/zigbee/zigbee-faq/ [Accessed 19 June 2023].

CVE (N.D.a) Thread Project. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-18345/product_id-46709/Thread-Project-Thread.html [Accessed 11 May 2023].

CVE (N.D.b) Bluetooth. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-11436/Bluetooth.html [Accessed 11 May 2023].

Danbatta, S. J. & Varol, A. (2019) 'Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation', *7th International Symposium on Digital Forensics and Security.* Barcelos, Portugal, 10-12 June. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/8757472 [Accessed 19 April 2023].

Darroudi, S. M. & Gomez, C. (2017) Bluetooth low energy mesh networks: A survey. *Sensors* 17(7): 1467. Available from: https://www.mdpi.com/1424-8220/17/7/1467 [Accessed 20 April 2023].

Dasgupta, A., Gill, A. Q. & Hussain F. (2019) 'Privacy of IoT-Enabled Smart Home Systems', in: Ismail, Y. (eds) *Internet of Things (IoT) for Automated and Smart Applications.* IntechOpen. 9-24. Available from: https://mts.intechopen.com/storage/books/7602/authors_book/authors_book.pdf [Accessed 30 March 2023].

Ding, J., Li, T. R. & Chen, X. L. (2018) The application of Wifi technology in smart home. *Journal of Physics: Conference Series* 1061(1): 012010. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1061/1/012010/meta [Accessed 19 April 2023].

Dorobantu, O. G. & Halunga, S. (2020) 'Security threats in IoT', *International Symposium on Electronics and Telecommunications.* Timisoara, Romania, 05-06 June. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/9301127 [Accessed 08 May 2023].

DSTIKE (N.D.) DSTIKE WiFI Deauther MiNi V3. Available from: https://dstike.com/products/dstike-wifi-deauther-mini [Accessed 13 July 2023].

El Jaouhari, S., Jose Palacios-Garcia, E., Anvari-Moghaddam, A. & Bouabdallah, A. (2019) Integrated management of energy, wellbeing and health in the next generation of smart homes. *Sensors* 19(3): 481. Available from: https://www.mdpi.com/1424-8220/19/3/481 [Accessed 24 April 2023].

Emami-Naeini, P., Dixon, H., Agarwal, Y. & Cranor, L. F. (2019) 'Exploring how privacy and security factor into IoT device purchase behavior', *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* Glasgow, Scotland, 04-09 May. New York, Association for Computing Machinery. 1-12. Available from: https://dl.acm.org/doi/abs/10.1145/3290605.3300764 [Accessed 08 May 2023].

Espressif Systems (2023) ESP32-S3 – ESP-IDF Programming Guide. Available from: https://docs.espressif.com/projects/esp-idf/en/latest/esp32s3/esp-idf-en-v5.2-dev-1805-g9a1cc59338-esp32s3.pdf [Accessed 23 July 2023].

Gomez, C., Oller, J. & Paradells, J. (2012) Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* 12(9): 11734-11753. Available from: https://www.mdpi.com/1424-8220/12/9/11734 [Accessed 20 April 2023].

Gupta, A. (2019) *The IoT Hacker's Handbook*. Berkeley, CA: Apress. Available from: https://learning.oreilly.com/library/view/the-iot-hackers/9781484243008/ [Accessed 24 March 2023].

Hameed, A. & Alomary, A. (2019) 'Security issues in IoT: A survey', *International conference on innovation and intelligence for informatics, computing, and technologies*. Sakhier, Bahrain, 22-23 September. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/8910320 [Accessed 31 July 2023].

Hazra, A., Adhikari, M., Amgoth, T. & Srirama, S. N. (2021) A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. *ACM Computing Surveys* 55(1): 1-35. Available from: https://dl.acm.org/doi/abs/10.1145/3485130 [Accessed 24 April 2023].

Heater, B. (2019) Amazon, Apple, Google and Zigbee join forces for an open smart home standard. *Techcrunch*. Available from: https://techcrunch.com/2019/12/18/amazon-apple-google-and-zigbee-join-forces-for-an-open-smart-home-standard/?guccounter=1&guce_referrer=aHR0cHM6Ly9kZS53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAMNaRe4lUPYn2zI24yRH3mZgqsLrkCDg6qKJHDeXfK0yKf3RuTrFkyFU3ceAwSgk_npWNH9bUd7FRVZr9xhDRYA3sIX5pFTUo81KeLx1t8faL1Za2sLRx7

N6toYV0WKGrvZGvR-WvyAy6J9U7PNikJH1kgJt3ehPIxVXAGV9YRrx [Accessed 06 April 2023].

Herrero, R. (2022) *Fundamentals of IoT Communication Technologies*. Cham: Springer. Available from: https://link.springer.com/content/pdf/10.1007/978-3-030-70080-5.pdf [Accessed 21 April 2023].

Higginbotham, S. (2021) Forget Cryptocurrencies and NFTs—Securing Devices Is the Future of Blockchain Technology. *IEEEE Spectrum*. Available from: https://spectrum.ieee.org/forget-cryptocurrencies-and-nftssecuring-devices-is-the-future-of-blockchain-technology [Accessed 04 May 2023].

Hollister, S. (January 23, 2019) No, Nest Cams are not being hacked to issue fake nuclar bomb threats. *The Verge*. Available from: https://www.theverge.com/2019/1/22/18193721/nest-cam-hack-north-korea-ballistic-missile-nuclear-threat-debunk [Accessed 03 April 2023].

Holz, T. (2022) Why is the Internet of Things So Hard to Secure? *Keyfactor*. Available from: https://www.keyfactor.com/blog/why-is-the-internet-of-things-so-hard-to-secure/ [Accessed 04 April 2023].

IEEE 802 LAN/MAN Standards Committee (2009) IEEE Standard for Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment1: Radio Resource Measurement of Wireless LANs. Available from: https://ieeexplore.ieee.org/document/5278657 [Accessed 22 July 2023].

IEEE Standards Association (2021) IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Available from: https://standards.ieee.org/ieee/802.11/7028/ [Accessed 13 April 2023].

International Business Machines Corporation & Eurotech (2015) MQTT V3.1 Protocol Specification. Available from: https://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html [Accessed 19 June 2023].

ISO (2015) ISO/IEC 2382:2015. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v2:en [Accessed 07 April 2023].

Kajor, M., Siu, I., Turon, M., Litvin, A., Zbarsky, B., Lunde, G. S., & Smith, M. (2023) Working with the CHIP Tool. Available from: https://github.com/project-chip/connectedhomeip/blob/master/docs/guides/chip_tool_guide.md [Accessed 13 July 2023].

Kalantar, G., Mohammadi, A. & Sadrieh, S. N. (2018) 'Analyzing the effect of Bluetooth low energy (BLE) with randomized MAC addresses in IoT applications', *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications*

(GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData. Halifax, Canada, 30 July - 03 August. IEEE. 27-34. Available from: https://ieeexplore.ieee.org/abstract/document/8726525 [Accessed 20 July 2023].

Khanji, S., Iqbal, F. & Hung, P. (2019) 'ZigBee security vulnerabilities: Exploration and evaluating', *10th international conference on information and communication systems.* Irbid, Jordan, 11-13 June. IEEE. 52-57. Available from: https://ieeexplore.ieee.org/abstract/document/8809115 [Accessed 17 June 2023].

Kirichek, R., Vishnevsky, V. & Koucheryavy, A. (2020) 'Analytic model of a mesh topology based on LoRa technology', *22nd International Conference on Advanced Communication Technology.* Phoenix Park, South Korea, 16-19 February. IEEE. 251-255. Available from: https://ieeexplore.ieee.org/abstract/document/9061519 [Accessed 19 April 2023].

Kismet (N.D.) Passive Capture. Available from: https://www.kismetwireless.net/docs/readme/intro/passive_capture/ [Accessed 24 July 2023].

Krasnyansky, M. (N.D.) sdptool (1) – Linux man page. Available from: https://linux.die.net/man/1/sdptool [Accessed 14 July 2023].

Kristiyanto, Y. & Ernastuti, E. (2020) Analysis of deauthentication attack on ieee 802.11 connectivity based on iot technology using external penetration test. *Communication and Information Technology Journal* 14(1): 45-51. Available from: https://journal.binus.ac.id/index.php/commit/article/view/6337/3826 [Accessed 13 June 2023].

Kumar, S. & Rai, S. (2012) Survey on transport layer protocols: TCP & UDP. *International Journal of Computer Applications 46*(7): 20-25. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ac50f6aeb6a5372f85cf05dab2a229b97a084555 [Accessed 25 April 2023].

Lamers, E., Dijksman, R., van der Vegt, A., Sarode, M. & de Laat, C. (2021) 'Securing home Wi-Fi with WPA3 personal', *IEEE 18th Annual Consumer Communications & Networking Conference.* Las Vegas, USA, 09-12 January. IEEE. 1-8. Available from: https://ieeexplore.ieee.org/abstract/document/9369629 [Accessed 23 July 2023].

Long, S. & Miao, F. (2019) 'Research on ZigBee wireless communication technology and its application', *IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference.* Chengdu, China, 20-22 December. IEEE. 1830-1834. Available from: https://ieeexplore.ieee.org/abstract/document/8997928 [Accessed 31 July 2023].

Lounis, K., Ding, S. H. & Zulkernine, M. (2021) 'Cut It: Deauthentication attacks on protected management frames in WPA2 and WPA3', in: Aïmeur, E., Laurent, M., Yaich, R., Dupont, B., Garcia-Alfaro, J. (eds) *Foundations and Practice of Security*. Springer. 235-252. Available from: https://link.springer.com/chapter/10.1007/978-3-031-08147-7_16 [Accessed 22 July 2023].

Maher, J. (September 23, 2019) Hacker Takes Over Couple's Smart Home, Plays Vulgar Music And Raises Temperature to 90 Degrees. *Newsweek*. Available from: https://www.newsweek.com/google-nest-hack-milwaukee-1460806 [Accessed 03 April 2023].

Margaritelli, S., Braga, G., Trotta, G. & Gruber, K. (2021) bettercap. Available from: https://github.com/bettercap/bettercap [Accessed 14 July 2023].

Marksteiner, S., Jimenez, V. J. E., Valiant, H. & Zeiner, H. (2017) 'An overview of wireless IoT protocol security in the smart home domain', *Internet of Things Business Models, Users, and Networks*. Copenhagen, Denmark, 23-24 November. IEEE. 1-8. Available from: https://ieeexplore.ieee.org/abstract/document/8260940 [Accessed 21 April 2023].

Mewada, S., Sharma, P. & Gautam, S. S. (2016) 'Exploration of efficient symmetric AES algorithm', *Symposium on Colossal Data Analysis and Networking.* Indore, India, 18-19 March. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/7570921 [Accessed 20 April 2023].

Miller, A. C. & Estrella, M. (2018) hcitool. Available from: https://github.com/MillerTechnologyPeru/hcitool [Accessed 14 July 2023].

Mogbil, R., Asqah, M. & Khediri, S. (2020) 'Iot: Security challenges and issues of smart homes/cities', *International Conference on Computing and Information Technology.* Univeristy of Tabuk, Sudi Arabia. 9-10 September. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/9213827 [Accessed 09 May 2023].

Nguyen, K., Golam Kibria, M., Ishizu, K. & Kojima, F. (2019) Performance evaluation of IEEE 802.11 ad in evolving Wi-Fi networks. Available from: https://www.hindawi.com/journals/wcmc/2019/4089365/ [Accessed 31 May 2023].

NIST (2022) NIST Transitioning Away from SHA-1 for All Applications. Available from: https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps [Accessed 03 May 2023].

Noman, H. A., Abdullah, S. M. & Mohammed, H. I. (2015) An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks. *International Journal of Computer Science Issues* 12(4): 107-112. Available from: https://www.researchgate.net/profile/Haydar-Mohammed/publication/283354063_An_Automated_Approach_to_Detect_Deauthentication_and_Disassociation_Dos_Attacks_on_Wireless_80211_Networks/links/563729f508ae758841151f49/An-Automated-Approach-to-Detect-Deauthentication-and-Disassociation-Dos-Attacks-on-Wireless-80211-Networks.pdf [Accessed 13 June 2023].

Nordic (2022) nRF Sniffer for Bluetooth LE v4.1.x. Available from: https://infocenter.nordicsemi.com/pdf/nRF_Sniffer_BLE_UG_v4.1.x.pdf [Accessed 17 July 2023].

Nordic (2023) Matter network overview. Available from: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.1.2/nrf/ug_matter_overview_network_topologies.html [Accessed 31 July 2023].

Noura, M., Atiquzzaman, M. & Gaedke, M. (2019) Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications 24*: 796-809. Available from: https://link.springer.com/article/10.1007/s11036-018-1089-9 [Accessed 24 April 2023].

OCF (2022) OCF Core Specification. Available from: https://openconnectivity.org/specs/OCF_Core_Specification.pdf [Accessed 24 April 2023].

OCF (N.D.) OCF SOLVING THE IOT STANDARDS GAP. Available from: https://openconnectivity.org/ [Accessed 24 April 2023].

Oliveira, L., Rodrigues, J. J., Kozlov, S. A., Rabêlo, R. A. & Albuquerque, V. H. C. D. (2019) MAC layer protocols for Internet of Things: A survey. *Future Internet* 11(1): 1-42. Available from: https://www.mdpi.com/1999-5903/11/1/16 [Accessed 31 May 2023].

Patil, S., Litvin, A., Jadhav, R., Zbarsky, B., Chen, S., Qixiang, W. & Wood, J. (2023) Matter ESP32 Lighting Example. Available from: https://github.com/project-chip/connectedhomeip/tree/master/examples/lighting-app/esp32 [Accessed 13 July 2023].

Pedhadiya, M. K., Jha, R. K. & Bhatt, H. G. (2019) Device to device communication: A survey. *Journal of Network and Computer Applications* 129(1): 71-89. Available from: https://www.sciencedirect.com/science/article/pii/S1084804518303345 [Accessed 01 September 2023].

Phan, L. A. & Kim, T. (2020) Breaking down the compatibility problem in smart homes: A dynamically updatable gateway platform. *Sensors* 20(10): 2783. Available from: https://www.mdpi.com/1424-8220/20/10/2783 [Accessed 18 April 2023].

Qureshi, I. A. & Asghar, S. (2023) A Systematic Review of the IEEE-802.11 Standard's Enhancements and Limitations. *Wireless Personal Communications* 131: 1-34. Available from: https://link.springer.com/article/10.1007/s11277-023-10553-7 [Accessed 22 July 2023].

Randewich, N. (July 15, 2014) Google's Nest launches network technology for connected home. *Reuters*. Available from: https://www.reuters.com/article/us-google-nest-idUSKBN0FK0JX20140715 [Accessed 09 May 2023].

Rzepecki, W. & Ryba, P. (2019) 'Iotsp: Thread mesh vs other widely used wireless protocols–comparison and use cases study', *7th International Conference on Future Internet of Things and Cloud.* Istanbul, Turkey, 26-28 August. IEEE. 291-295. Available from: https://ieeexplore.ieee.org/abstract/document/8972835 [Accessed 09 May 2023].

Rzepecki, W., Iwanecki, Ł. & Ryba, P. (2018) 'IEEE 802.15. 4 thread mesh network–data transmission in harsh environment', *6th International Conference on Future Internet of*

Things and Cloud Workshops. Barcelona, Spain, 06-08 August. IEEE. 42-47. Available from: https://ieeexplore.ieee.org/abstract/document/8488173 [Accessed 31 July 2023].

Samuel, S. S. I. (2016) 'A review of connectivity challenges in IoT-smart home', *3rd MEC International conference on big data and smart city.* Muscat, Oman, 15-16 March. IEEE. 1-4. Available from: https://ieeexplore.ieee.org/abstract/document/7460395 [Accessed 19 April 2023].

Scapy (N.D.) What is Scapy? Available from: https://scapy.net/ [Accessed 13 July 2023].

Scheible, T. (2020) Spionage von Bluetooth-Verbindungen. Available from: https://scheible.it/bluetooth-spionage/ [Access 21 July 2023].

SecWiki (N.D.) Npcap/WiFi adapters. Available from: https://secwiki.org/w/Npcap/WiFi_adapters [Accessed 24 July 2023].

Shripad621git (2023) OnMessageReceived failed, err = 70 (CON-571) #468. Available from: https://github.com/espressif/esp-matter/issues/468 [Accessed 24 July 2023].

Soni, D. & Makwana, A. (2017) 'A survey on mqtt: a protocol of internet of things (iot)', *International conference on telecommunication, power analysis and computing techniques.* Chennai, India, 12 April. Research Gate. 173-177. Available from: https://www.researchgate.net/profile/Dipa-Soni/publication/316018571_A_SURVEY_ON_MQTT_A_PROTOCOL_OF_INTERNET_OF_THINGSIOT/links/58edafd4aca2724f0a26e0bf/A-SURVEY-ON-MQTT-A-PROTOCOL-OF-INTERNET-OF-THINGSIOT.pdf [Accessed 19 June 2023].

Statista (2022) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. Available from: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [Accessed 04 April 2023].

Sung, T. W., Wu, T. T., Yang, C. S. & Huang, Y. M. (2010) Reliable data broadcast for zigbee wireless sensor networks. *International journal on smart sensing and intelligent systems* 3(3): 504-520. Available from: https://sciendo.com/article/10.21307/ijssis-2017-405 [Accessed 31 July 2023].

Thread Group (N.D.) What is Thread?. Available from: https://www.threadgroup.org/What-is-Thread/Overview [Accessed 21 April 2023].

Tightiz, L. & Yang, H. (2020) A comprehensive review on IoT protocols' features in smart grid communication. *Energies* 13(11): 1-24. Available from: https://www.mdpi.com/1996-1073/13/11/2762 [Accessed 18 April 2023].

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F. & Bilal, M. (2021) Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* 77(12): 1453-14089. Available from: https://link.springer.com/article/10.1007/s11227-021-03825-1 [Accessed 02 September 2023].

Unwala, I., Taqvi, Z. & Lu, J. (2018) 'Thread: An iot protocol', *IEEE Green Technologies Conference.* Austin, Texas, 07 June. IEEE. 161-167. Available from: https://ieeexplore.ieee.org/abstract/document/8373620 [Accessed 21 April 2023].

Valtchev, D. & Frankov, I. (2002) Service gateway architecture for a smart home. *IEEE Communications Magazine* 40(4): 126-132. Available from: https://ieeexplore.ieee.org/abstract/document/995862 [Accessed 24 April 2023].

Vanhoef, M. & Piessens, F. (2018) 'Release the Kraken: new KRACKs in the 802.11 Standard', *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* Toronto, Canada, 15-19 October. New York, Association for Computing Machinery. 299-314. Available from: https://dl.acm.org/doi/abs/10.1145/3243734.3243807 [Accessed 19 April 2023].

Wi-Fi Alliance (2010) Wi-Fi certified Wi-Fi Direct. Available from: https://www.wi-fi.org/system/files/wp_Wi-Fi_Direct_20101025_Industry.pdf [Accessed 19 April 2023].

WikiDevi (2021) List of Wiresless Adapters That Support Monitor Mode and Packet Injection. Available from: https://deviwiki.com/wiki/List_of_Wireless_Adapters_That_Support_Monitor_Mode_and_Packet_Injection [Accessed 24 July 2023].

Wireshark Foundation (N.D) The world's most popular network protocol analyzer. Available from: https://www.wireshark.org/ [Accessed 31 July 2023].

Wollinger, G. R., Dreißigacker, A., Blauert, K., Bartsch, T. & Baier, D. (2014) Wohnungseinbruch: Tat und Folgen. Kriminologische Forschungsinstitut Niedersachsen e.V. Available from: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_124.pdf [Accessed 04 April 2023].

Woolf, N. (October 26, 2016) DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*. Available from: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [Accessed 04 April 2023].

Yuan, M. (2021) Getting to know MQTT. Available from: https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/ [Accessed 19 June 2023].

Zhang, X., Upton, O., Beebe, N. L. & Choo, K. K. R. (2020) Iot botnet forensics: A comprehensive digital forensic case study on mirai botnet servers. *Forensic Science International: Digital Investigation 32*: 300926. Available from: https://www.sciencedirect.com/science/article/pii/S2666281720300214 [Accessed 04 April 2023].

Zigbee Alliance (2016) Base Device Behavior Specification Version 1.0. Available from: https://csa-iot.org/wp-content/uploads/2022/01/docs-13-0402-13-00zi-Base-Device-Behavior-Specification.pdf [Accessed 18 June 2023].

Zohourian, A., Dadkhah, S., Neto, E. C. P., Mahdikhani, H., Danso, P. K., Molyneaux, H. & Ghorbani, A. A. (2023) IoT Zigbee device security: A comprehensive review. *Internet of Things*, 22: 100791. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2542660523001142 [Accessed 18 June 2023].

Appendices

1. Installation of Matter and creation of the Matter ESP32 microcontroller

Command	Description
$ sudo apt install python pip cmake git	Basic prerequisites
$ git clone -b v4.4.4 --recursive https://github.com/espressif/esp-idf.git	Clone of the ESP-IDF Github repository.
$ sudo apt-get install git wget flex bison gperf python3 python3-pip python3-venv cmake ninja-build ccache libffi-dev libssl-dev dfu-util libusb-1.0-0	ESP-IDF prerequisites for Ubuntu and Debian OS.
$ cd /…/esp-idf $ ./install.sh $. ./export.sh	Setup of the ESP-IDF.
$ sudo apt-get install git gcc g++ pkg-config libssl-dev libdbus-1-dev \ libglib2.0-dev libavahi-client-dev ninja-build python3-venv python3-dev \ python3-pip unzip libgirepository1.0-dev libcairo2-dev libreadline-dev	Matter prerequisites
$ git clone –recurse-submodules https://github.com/project-chip/connectedhomeip.git	Clone of the Matter Github repository.
$ cd /.../connectedhomeip $ source scripts/activate.sh	Activation of the Matter environment.

$ cd /.../connectedhomeip/examples/lighting-app/esp32
$ idf.py set-target ESP32-S3
$ idf.py menuconfig
$ idf.py build
	Build of the lighting-app application for the ESP32-S3 microcontroller was used. The *menuconfig* command allows to make changes of the settings of the application. However the target device of the ESP32 series can only determined with the *set-target* promt.

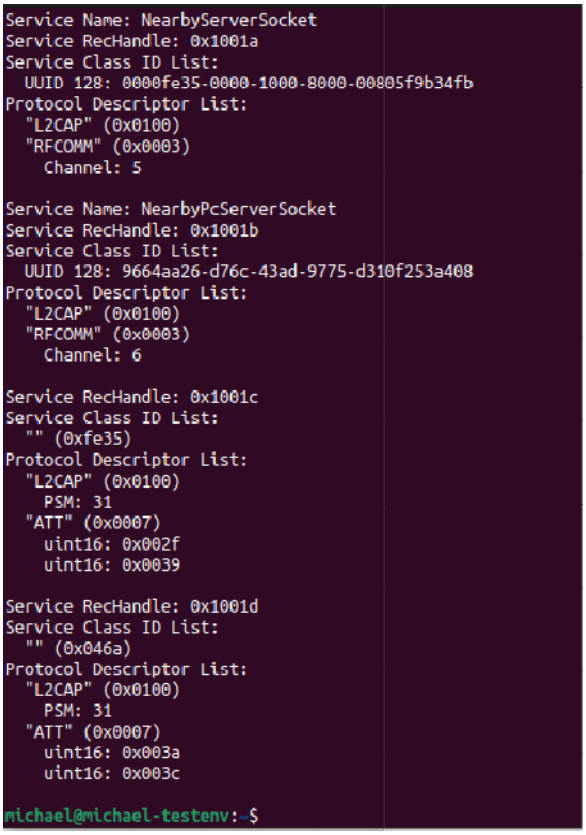
$ sudo chmod a+rw /dev/ttyUSB0	Enable permission for the /dev/ttyUSB0 port to allow flashing of the microcontroller.

$ cd /.../connectedhomeip/examples/lighting-app/esp32
$ idf.py –p /dev/ttyUSB0 erase-flash
$ idf.py –p /dev/ttyUSB0 flash
$ idf.py –p /dev/ttyUSB0 monitor
	Flashing of the microcontroller. To guarantee a successful flashing process, older applications on the microcontroller should be deleted. With the *monitor* command it is possible to check the successful flashing.

2. Further device information via the sdptool

```
michael@michael-testenv:~$ sdptool browse 1C:B7:96:38:8F:67
Browsing 1C:B7:96:38:8F:67 ...
Service RecHandle: 0x10000
Service Class ID List:
  "Generic Attribute" (0x1801)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0001
    uint16: 0x0003

Service RecHandle: 0x10001
Service Class ID List:
  "Generic Access" (0x1800)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0014
    uint16: 0x001a

Service Name: BrManagerInsecure
Service RecHandle: 0x1000f
Service Class ID List:
  UUID 128: 8ce255c0-200a-11e0-ac64-0800200c9a66
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 4

Service Name: Headset Gateway
Service RecHandle: 0x10010
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 2
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0102

Service Name: Handsfree Gateway
Service RecHandle: 0x10011
Service Class ID List:
  "Handsfree Audio Gateway" (0x111f)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 3
Profile Descriptor List:
  "Handsfree" (0x111e)
    Version: 0x0106

Service Name: AV Remote Control Target
Service RecHandle: 0x10012
Service Class ID List:
  "AV Remote Target" (0x110c)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 23
  "AVCTP" (0x0017)
    uint16: 0x0103
Profile Descriptor List:
  "AV Remote" (0x110e)
    Version: 0x0104

Service Name: Advanced Audio Source
Service RecHandle: 0x10013
Service Class ID List:
  "Audio Source" (0x110a)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 25
  "AVDTP" (0x0019)
    uint16: 0x0103
Profile Descriptor List:
  "Advanced Audio" (0x110d)
    Version: 0x0103
```

```
Service Name: Android Network Access Point
Service Description: NAP
Service RecHandle: 0x10014
Service Class ID List:
  "Network Access Point" (0x1116)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 15
  "BNEP" (0x000f)
    Version: 0x0100
    SEQ8: 0 6
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Network Access Point" (0x1116)
    Version: 0x0100

Service Name: Android Network User
Service Description: PANU
Service RecHandle: 0x10015
Service Class ID List:
  "PAN User" (0x1115)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 15
  "BNEP" (0x000f)
    Version: 0x0100
    SEQ8: 0 6
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "PAN User" (0x1115)
    Version: 0x0100

Service Name: SMS/MMS
Service RecHandle: 0x10016
Service Class ID List:
  "Message Access - MAS" (0x1132)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 26
  "OBEX" (0x0008)
Profile Descriptor List:
  "Message Access" (0x1134)
    Version: 0x0102

Browsing 1C:B7:96:38:8F:67 ...
Service Search failed: Invalid argument
Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x10017
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 19
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0101

Service Name: OBEX Object Push
Service RecHandle: 0x10018
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0102

Browsing 1C:B7:96:38:8F:67 ...
Service Search failed: Invalid argument
Service RecHandle: 0x10019
Service Class ID List:
  UUID 128: 11c8b310-80e4-4276-afc0-f81590b2177f
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0028
    uint16: 0x002e
```


Service Name: NearbyServerSocket
Service RecHandle: 0x1001a
Service Class ID List:
UUID 128: 0000fe35-0000-1000-8000-00805f9b34fb
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 5
Service Name: NearbyPcServerSocket
Service RecHandle: 0x1001b
Service Class ID List:
UUID 128: 9664aa26-d76c-43ad-9775-d310f253a408
Protocol Descriptor List:
"L2CAP" (0x0100)
"RFCOMM" (0x0003)
Channel: 6
Service RecHandle: 0x1001c
Service Class ID List:
"" (0xfe35)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 31
"ATT" (0x0007)
uint16: 0x002f
uint16: 0x0039
Service RecHandle: 0x1001d
Service Class ID List:
"" (0x046a)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 31
"ATT" (0x0007)
uint16: 0x003a
uint16: 0x003c
michael@michael-testenv:~$

3. Complete Wireshark scan protocol of the commissioning process of the Apple Watch

Number	Time	Source	Protocol	Length	Delta time	Sequence number	More data	Event counter	Info
1	0.000	Master	LE LL	6		0	False	0	Control Opcode: LL_VERSION_IND
2	0.000	Slave	LE LL	0	149µs	0	True	0	Empty PDU
3	0.000	Master	LE LL	0	151µs	1	False	0	Empty PDU
4	0.030	Master	LE LL	0	29412µs	1	False	1	Empty PDU
5	0.030	Slave	LE LL	6	149µs	1	True	1	Control Opcode: LL_VERSION_IND
6	0.030	Master	LE LL	0	151µs	0	False	1	Empty PDU
7	0.030	Slave	LE LL	9	149µs	0	True	1	Control Opcode: LL_SLAVE_FEATURE_REQ
8	0.031	Master	LE LL	0	151µs	1	True	1	Empty PDU
9	0.031	Slave	LE LL	0	149µs	1	False	1	Empty PDU
10	0.031	Master	LE LL	6	151µs	0	False	1	Control Opcode: Unknown
11	0.031	Slave	LE LL	0	149µs	0	False	1	Empty PDU
12	0.059	Master	LE LL	9	28143µs	1	False	2	Control Opcode: LL_FEATURE_RSP
13	0.060	Slave	LE LL	2	150µs	1	True	2	Control Opcode: LL_UNKNOWN_RSP
14	0.060	Master	LE LL	0	150µs	0	False	2	Empty PDU
15	0.090	Master	LE LL	0	29373µs	0	True	3	Empty PDU
16	0.090	Slave	LE LL	0	150µs	0	False	3	Empty PDU
17	0.090	Master	LE LL	6	150µs	1	False	3	Control Opcode: Unknown
18	0.090	Slave	LE LL	0	150µs	1	False	3	Empty PDU
19	0.120	Master	LE LL	0	29183µs	0	False	4	Empty PDU
20	0.120	Slave	LE LL	6	150µs	0	True	4	Control Opcode: Unknown
21	0.120	Master	LE LL	0	150µs	1	False	4	Empty PDU
22	0.120	Slave	LE LL	0	150µs	1	False	4	Empty PDU
23	0.150	Master	LE LL	3	29182µs	0	False	5	Control Opcode: LL_PHY_REQ
24	0.150	Slave	LE LL	0	150µs	0	False	5	Empty PDU
25	0.180	Master	LE LL	0	29667µs	1	False	6	Empty PDU
26	0.180	Slave	LE LL	3	150µs	1	True	6	Control Opcode: LL_PHY_RSP
27	0.180	Master	LE LL	0	150µs	0	False	6	Empty PDU
28	0.180	Slave	LE LL	0	150µs	0	False	6	Empty PDU
29	0.210	Master	LE LL	5	29206µs	1	False	7	Control Opcode: LL_PHY_UPDATE_IND
30	0.210	Slave	LE LL	0	150µs	1	False	7	Empty PDU
31	0.240	Master	LE LL	0	29649µs	0	False	8	Empty PDU
32	0.240	Slave	LE LL	0	150µs	0	False	8	Empty PDU
33	0.270	Master	LE LL	0	29691µs	1	False	9	Empty PDU
34	0.270	Slave	LE LL	0	150µs	1	False	9	Empty PDU
35	0.300	Master	LE LL	0	29692µs	0	False	10	Empty PDU
36	0.300	Slave	LE LL	0	150µs	0	False	10	Empty PDU
37	0.330	Master	LE LL	0	29689µs	1	False	11	Empty PDU
38	0.330	Slave	LE LL	0	150µs	1	False	11	Empty PDU
39	0.360	Master	LE LL	0	29691µs	0	False	12	Empty PDU
40	0.360	Slave	LE LL	0	149µs	0	False	12	Empty PDU
41	0.390	Master	LE LL	0	29693µs	1	False	13	Empty PDU
42	0.390	Slave	LE LL	0	150µs	1	False	13	Empty PDU

43	0.420	Master	LE LL	0	29687µs	0	False	14	Empty PDU
44	0.420	Slave	LE LL	0	151µs	0	False	14	Empty PDU
45	0.450	Master	LE LL	9	29763µs	1	False	15	Control Opcode: LL_FEATURE_REQ
46	0.450	Slave	LE LL	0	149µs	1	False	15	Empty PDU
47	0.480	Master	LE LL	0	29726µs	0	False	16	Empty PDU
48	0.480	Slave	LE LL	9	150µs	0	True	16	Control Opcode: LL_FEATURE_RSP
49	0.480	Master	LE LL	0	150µs	1	False	16	Empty PDU
50	0.480	Slave	LE LL	0	150µs	1	False	16	Empty PDU
51	0.510	Master	LE LL	9	29339µs	0	False	17	Control Opcode: LL_LENGTH_REQ
52	0.510	Slave	LE LL	0	150µs	0	False	17	Empty PDU
53	0.540	Master	LE LL	0	29727µs	1	False	18	Empty PDU
54	0.540	Slave	LE LL	9	149µs	1	True	18	Control Opcode: LL_LENGTH_RSP
55	0.540	Master	LE LL	0	150µs	0	False	18	Empty PDU
56	0.540	Slave	LE LL	0	150µs	0	False	18	Empty PDU
57	0.570	Master	L2CAP	11	29339µs	1	True	19	
58	0.570	Slave	ATT	11	150µs	1	False	19	Rcvd Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0001..0xffff
59	0.570	Master	ATT	7	150µs	0	False	19	Sent Exchange MTU Request, Client Rx MTU: 527
60	0.570	Slave	LE LL	0	150µs	0	False	19	Empty PDU
61	0.600	Master	ATT	24	29258µs	1	False	20	Sent Read By Group Type Response, Attribute List Length: 3, Generic Access Profile, Generic Attribute Profile, Device Information
62	0.600	Slave	L2CAP	11	150µs	1	True	20	
63	0.600	Master	LE LL	0	150µs	0	False	20	Empty PDU
64	0.600	Slave	ATT	7	150µs	0	False	20	Rcvd Exchange MTU Response, Server Rx MTU: 527
65	0.630	Master	L2CAP	24	29206µs	1	True	21	
66	0.630	Slave	ATT	11	150µs	1	False	21	Rcvd Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x000f..0xffff
67	0.630	Master	ATT	11	149µs	0	False	21	Sent Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0001..0xffff
68	0.630	Slave	LE LL	0	150µs	0	False	21	Empty PDU
69	0.660	Master	ATT	46	29191µs	1	False	22	Sent Read By Group Type Response, Attribute List Length: 2, Unknown, Unknown
70	0.660	Slave	L2CAP	10	151µs	1	True	22	
71	0.660	Master	LE LL	0	149µs	0	False	22	Empty PDU
72	0.660	Slave	ATT	24	150µs	0	False	22	Rcvd Read By Group Type Response, Attribute List Length: 3, Generic Access Profile, Generic Attribute Profile, Device Information
73	0.690	Master	L2CAP	11	29056µs	1	True	23	
74	0.690	Slave	ATT	11	150µs	1	False	23	Rcvd Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0019..0xffff
75	0.690	Master	ATT	11	150µs	0	False	23	Sent Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x000f..0xffff
76	0.690	Slave	LE LL	0	150µs	0	False	23	Empty PDU
77	0.720	Master	ATT	18	29241µs	1	False	24	Sent Read By Group Type Response, Attribute List Length: 2, Battery Service, Current Time Service
78	0.720	Slave	LE LL	183	150µs	0	True	24	Control Opcode: Unknown
79	0.750	Master	LE LL	24	28959µs	0	True	25	Control Opcode: LL_CONNECTION_PARAM_REQ
80	0.750	Slave	LE LL	0	150µs	0	False	25	Empty PDU
81	0.750	Master	ATT	11	150µs	1	True	25	Sent Read By Group Type Request, GATT Primary Service Declaration, Handles:

									0x0023..0xffff
82	0.780	Master	ATT	11	29428µs	1	True	26	Sent Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0023..0xffff
83	0.780	Slave	LE LL	24	149µs	1	True	26	Control Opcode: LL_CONNECTION_PARAM_RSP
84	0.780	Master	LE LL	4	150µs	0	True	26	Control Opcode: Unknown
85	0.780	Slave	LE LL	0	149µs	0	False	26	Empty PDU
86	0.780	Master	ATT	46	150µs	1	True	26	Sent Read By Group Type Response, Attribute List Length: 2, Unknown, Unknown
87	0.810	Master	ATT	46	28843µs	1	True	27	Sent Read By Group Type Response, Attribute List Length: 2, Unknown, Unknown
88	0.810	Slave	ATT	9	150µs	1	False	27	Rcvd Error Response - Attribute Not Found, Handle: 0x0023 (Unknown)
89	0.810	Master	L2CAP	11	150µs	0	False	27	Connection oriented channel
90	0.810	Slave	LE LL	0	150µs	0	False	27	Empty PDU
91	0.840	Master	LE LL	12	29111µs	1	True	28	Control Opcode: LL_CONNECTION_UPDATE_IND
92	0.840	Slave	ATT	11	149µs	1	False	28	Rcvd Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0039..0xffff
93	0.840	Master	ATT	11	150µs	0	False	28	Sent Read By Type Request, Device Name, Handles: 0x0001..0x0005
94	0.870	Master	ATT	11	29434µs	0	True	29	Sent Read By Type Request, Device Name, Handles: 0x0001..0x0005
95	0.870	Slave	LE LL	0	149µs	0	False	29	Empty PDU
96	0.870	Master	ATT	9	150µs	1	False	29	Sent Error Response - Attribute Not Found, Handle: 0x0039 (Unknown: Unknown)
97	0.870	Slave	LE LL	0	149µs	1	False	29	Empty PDU
98	0.900	Master	LE LL	0	29295µs	0	False	30	Empty PDU
99	0.900	Slave	ATT	19	150µs	0	True	30	Rcvd Read By Type Response, Attribute List Length: 1
100	0.900	Master	LE LL	0	150µs	1	False	30	Empty PDU
101	0.900	Slave	ATT	11	150µs	1	False	30	Rcvd Read By Type Request, Device Name, Handles: 0x0001..0x0005
102	0.930	Master	ATT	11	29255µs	0	True	31	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0006..0x0009
103	0.930	Slave	LE LL	0	150µs	0	False	31	Empty PDU
104	0.930	Master	ATT	14	149µs	1	False	31	Sent Read By Type Response, Attribute List Length: 1
105	0.930	Slave	LE LL	0	150µs	1	False	31	Empty PDU
106	0.960	Master	LE LL	0	29275µs	0	False	32	Empty PDU
107	0.960	Slave	ATT	13	150µs	0	True	32	Rcvd Read By Type Response, Attribute List Length: 1, Service Changed
108	0.960	Master	LE LL	0	150µs	1	False	32	Empty PDU
109	0.960	Slave	ATT	11	150µs	1	False	32	Rcvd Read By Type Request, GATT Characteristic Declaration, Handles: 0x0006..0x0009
110	0.990	Master	ATT	13	29278µs	0	True	33	Sent Read By Type Response, Attribute List Length: 1, Service Changed
111	0.990	Slave	LE LL	0	149µs	0	False	33	Empty PDU
112	0.990	Master	ATT	9	151µs	1	False	33	Sent Find Information Request, Handles: 0x0009..0x0009
113	0.990	Slave	LE LL	0	149µs	1	False	33	Empty PDU
114	1.020	Master	LE LL	0	29288µs	0	False	34	Empty PDU
115	1.020	Slave	ATT	10	150µs	0	True	34	Rcvd Find Information Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
116	1.020	Master	LE LL	0	150µs	1	False	34	Empty PDU
117	1.020	Slave	ATT	9	150µs	1	False	34	Rcvd Find Information Request, Handles: 0x0009..0x0009
118	1.050	Master	ATT	9	29299µs	0	True	35	Sent Write Request, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
119	1.050	Slave	LE LL	0	150µs	0	False	35	Empty PDU

120	1.050	Master	ATT	10	150µs	1	False	35	Sent Find Information Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
121	1.050	Slave	LE LL	0	150µs	1	False	35	Empty PDU
122	1.080	Master	LE LL	0	29298µs	0	False	36	Empty PDU
123	1.080	Slave	ATT	5	150µs	0	True	36	Rcvd Write Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
124	1.080	Master	LE LL	0	150µs	1	False	36	Empty PDU
125	1.080	Slave	ATT	9	150µs	1	False	36	Rcvd Write Request, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
126	1.110	Master	ATT	5	29317µs	0	True	37	Sent Write Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
127	1.110	Slave	LE LL	0	150µs	0	False	37	Empty PDU
128	1.110	Master	ATT	11	150µs	1	False	37	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0019..0x0022
129	1.110	Slave	LE LL	0	150µs	1	False	37	Empty PDU
130	1.140	Master	LE LL	0	29311µs	0	False	38	Empty PDU
131	1.140	Slave	ATT	69	150µs	0	False	38	Rcvd Read By Type Response, Attribute List Length: 3, Unknown, Unknown, Unknown
132	1.170	Master	ATT	11	29486µs	1	False	39	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0021..0x0022
133	1.170	Slave	LE LL	0	149µs	1	False	39	Empty PDU
134	1.200	Master	LE LL	0	29719µs	0	False	40	Empty PDU
135	1.200	Slave	ATT	9	150µs	0	False	40	Rcvd Error Response - Attribute Not Found, Handle: 0x0022 (Battery Service: Unknown: Unknown)
136	1.230	Master	ATT	7	29728µs	1	False	41	Sent Read Request, Handle: 0x001e (Battery Service: Unknown)
137	1.230	Slave	LE LL	0	149µs	1	False	41	Empty PDU
138	1.260	Master	LE LL	0	29735µs	0	False	42	Empty PDU
139	1.260	Slave	ATT	27	149µs	0	False	42	Rcvd Read Response, Handle: 0x001e (Battery Service: Unknown)
140	1.290	Master	ATT	11	29654µs	1	False	43	Sent Write Request, Handle: 0x001b (Battery Service: Unknown)
141	1.290	Slave	LE LL	0	149µs	1	False	43	Empty PDU
142	1.320	Master	LE LL	0	29720µs	0	False	44	Empty PDU
143	1.320	Slave	LE LL	4	150µs	0	False	44	L2CAP Fragment Start
144	1.350	Master	LE LL	0	29746µs	1	False	45	Empty PDU
145	1.350	Slave	LE LL	0	150µs	1	False	45	Empty PDU
146	1.380	Master	LE LL	0	29763µs	0	False	46	Empty PDU
147	1.440	Master	LE LL	0	59956µs	0	False	48	Empty PDU
148	1.470	Master	LE LL	0	29956µs	0	False	49	Empty PDU
149	1.500	Master	LE LL	0	29956µs	0	False	50	Empty PDU
150	1.530	Master	LE LL	0	29956µs	0	False	51	Empty PDU
151	1.530	Slave	LE LL	0	150µs	0	False	51	Empty PDU
152	1.560	Master	LE LL	0	29763µs	1	False	52	Empty PDU
153	1.590	Master	LE LL	0	29956µs	1	False	53	Empty PDU
154	1.620	Master	LE LL	0	29957µs	1	False	54	Empty PDU
155	1.650	Master	LE LL	0	29956µs	1	False	55	Empty PDU
156	1.680	Master	LE LL	0	29956µs	1	False	56	Empty PDU
157	1.710	Master	LE LL	0	29958µs	1	False	57	Empty PDU

158	1.710	Slave	LE LL	0	149µs	1	False	57	Empty PDU
159	1.740	Master	LE LL	0	29762µs	0	False	58	Empty PDU
160	1.770	Master	LE LL	0	29957µs	0	False	59	Empty PDU
161	1.800	Master	LE LL	0	29956µs	0	False	60	Empty PDU
162	1.830	Master	LE LL	0	29956µs	0	False	61	Empty PDU
163	1.860	Master	LE LL	0	29957µs	0	False	62	Empty PDU
164	1.890	Master	LE LL	0	29956µs	0	False	63	Empty PDU
165	1.890	Slave	LE LL	0	150µs	0	False	63	Empty PDU
166	1.950	Master	LE LL	0	59763µs	1	False	65	Empty PDU
167	1.980	Master	LE LL	0	29957µs	1	False	66	Empty PDU
168	2.010	Master	LE LL	0	29956µs	1	False	67	Empty PDU
169	2.040	Master	LE LL	0	29957µs	1	False	68	Empty PDU
170	2.070	Master	LE LL	0	29956µs	1	False	69	Empty PDU
171	2.070	Slave	LE LL	0	149µs	1	False	69	Empty PDU
172	2.100	Master	LE LL	0	29764µs	0	False	70	Empty PDU
173	2.130	Master	LE LL	0	29956µs	0	False	71	Empty PDU
174	2.160	Master	LE LL	0	29957µs	0	False	72	Empty PDU
175	2.190	Master	LE LL	0	29956µs	0	False	73	Empty PDU
176	2.220	Master	LE LL	0	29956µs	0	False	74	Empty PDU
177	2.250	Master	LE LL	0	29958µs	0	False	75	Empty PDU
178	2.280	Master	LE LL	0	29956µs	1	False	76	Empty PDU
179	2.310	Master	LE LL	0	29955µs	1	False	77	Empty PDU
180	2.340	Master	LE LL	0	29957µs	1	False	78	Empty PDU
181	2.370	Master	LE LL	0	29957µs	1	True	79	Empty PDU
182	2.400	Master	LE LL	0	29955µs	1	True	80	Empty PDU
183	2.430	Master	LE LL	0	29957µs	1	True	81	Empty PDU
184	2.430	Slave	LE LL	0	150µs	1	False	81	Empty PDU
185	2.430	Master	LE LL	2	150µs	0	False	81	Control Opcode: LL_TERMINATE_IND
186	2.430	Slave	LE LL	0	149µs	0	False	81	Empty PDU

4. Complete Wireshark scan protocol of the commissioning process of the Matter device

Number	Time	Source	Protocol	Length	Delta time	Sequence number	More data	Event counter	Info
1	0.000	Master	LE LL	6		0	False	0	Control Opcode: LL_VERSION_IND
2	0.000	Slave	LE LL	9	151µs	0	True	0	Control Opcode: LL_SLAVE_FEATURE_REQ
3	0.000	Master	LE LL	0	150µs	1	False	0	Empty PDU
4	0.000	Slave	LE LL	0	151µs	1	False	0	Empty PDU
5	0.022	Master	LE LL	9	21609µs	0	False	1	Control Opcode: LL_FEATURE_RSP
6	0.022	Slave	LE LL	6	150µs	0	True	1	Control Opcode: LL_VERSION_IND
7	0.023	Master	LE LL	0	151µs	1	False	1	Empty PDU
8	0.023	Slave	LE LL	0	150µs	1	False	1	Empty PDU
9	0.045	Master	LE LL	3	21609µs	0	False	2	Control Opcode: LL_PHY_REQ
10	0.045	Slave	LE LL	0	151µs	0	False	2	Empty PDU
11	0.067	Master	LE LL	0	22166µs	1	False	3	Empty PDU
12	0.067	Slave	LE LL	3	151µs	1	True	3	Control Opcode: LL_PHY_RSP
13	0.067	Master	LE LL	0	150µs	0	False	3	Empty PDU
14	0.068	Slave	LE LL	0	151µs	0	False	3	Empty PDU
15	0.090	Master	LE LL	5	21704µs	1	False	4	Control Opcode: LL_PHY_UPDATE_IND
16	0.090	Slave	LE LL	0	151µs	1	False	4	Empty PDU
17	0.112	Master	LE LL	0	22149µs	0	False	5	Empty PDU
18	0.112	Slave	LE LL	0	150µs	0	False	5	Empty PDU
19	0.135	Master	LE LL	0	22190µs	1	False	6	Empty PDU
20	0.135	Slave	LE LL	0	150µs	1	False	6	Empty PDU
21	0.157	Master	LE LL	0	22191µs	0	False	7	Empty PDU
22	0.157	Slave	LE LL	0	151µs	0	False	7	Empty PDU
23	0.180	Master	LE LL	0	22189µs	1	False	8	Empty PDU
24	0.180	Slave	LE LL	0	151µs	1	False	8	Empty PDU
25	0.202	Master	LE LL	0	22190µs	0	False	9	Empty PDU
26	0.202	Slave	LE LL	0	150µs	0	False	9	Empty PDU
27	0.225	Master	LE LL	0	22190µs	1	False	10	Empty PDU
28	0.225	Slave	LE LL	0	150µs	1	False	10	Empty PDU
29	0.247	Master	LE LL	0	22187µs	0	False	11	Empty PDU
30	0.247	Slave	LE LL	0	150µs	0	False	11	Empty PDU
31	0.270	Master	LE LL	9	22264µs	1	False	12	Control Opcode: LL_LENGTH_REQ
32	0.270	Slave	LE LL	0	150µs	1	False	12	Empty PDU
33	0.292	Master	LE LL	0	22226µs	0	False	13	Empty PDU
34	0.292	Slave	LE LL	9	150µs	0	True	13	Control Opcode: LL_LENGTH_RSP
35	0.292	Master	LE LL	0	150µs	1	False	13	Empty PDU
36	0.293	Slave	LE LL	0	150µs	1	False	13	Empty PDU
37	0.315	Master	ATT	7	21838µs	0	False	14	Sent Exchange MTU Request, Client Rx MTU: 527
38	0.315	Slave	LE LL	0	150µs	0	False	14	Empty PDU
39	0.337	Master	LE LL	0	22235µs	1	False	15	Empty PDU
40	0.337	Slave	ATT	7	149µs	1	True	15	Rcvd Exchange MTU Response, Server Rx MTU: 256
41	0.337	Master	LE LL	0	151µs	0	False	15	Empty PDU
42	0.338	Slave	LE LL	0	149µs	0	False	15	Empty PDU

43	0.360	Master	ATT	11	21847µs	1	False	16	Sent Read By Group Type Request, GATT Primary Service Declaration, Handles: 0x0001..0xffff
44	0.360	Slave	LE LL	0	150µs	1	False	16	Empty PDU
45	0.382	Master	LE LL	0	22217µs	0	False	17	Empty PDU
46	0.382	Slave	ATT	24	150µs	0	True	17	Rcvd Read By Group Type Response, Attribute List Length: 3, Generic Access Profile, Generic Attribute Profile, ZigBee Alliance
47	0.382	Master	LE LL	0	150µs	1	False	17	Empty PDU
48	0.383	Slave	LE LL	0	150µs	1	False	17	Empty PDU
49	0.405	Master	ATT	11	21778µs	0	False	18	Sent Read By Type Request, Device Name, Handles: 0x0001..0x0005
50	0.405	Slave	LE LL	0	150µs	0	False	18	Empty PDU
51	0.427	Master	LE LL	0	22219µs	1	False	19	Empty PDU
52	0.427	Slave	ATT	19	150µs	1	True	19	Rcvd Read By Type Response, Attribute List Length: 1
53	0.427	Master	LE LL	0	150µs	0	False	19	Empty PDU
54	0.428	Slave	LE LL	0	150µs	0	False	19	Empty PDU
55	0.450	Master	ATT	11	21799µs	1	False	20	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x0006..0x0009
56	0.450	Slave	LE LL	0	150µs	1	False	20	Empty PDU
57	0.472	Master	LE LL	0	22219µs	0	False	21	Empty PDU
58	0.472	Slave	ATT	13	149µs	0	True	21	Rcvd Read By Type Response, Attribute List Length: 1, Service Changed
59	0.472	Master	LE LL	0	151µs	1	False	21	Empty PDU
60	0.473	Slave	LE LL	0	149µs	1	False	21	Empty PDU
61	0.495	Master	ATT	9	21822µs	0	False	22	Sent Find Information Request, Handles: 0x0009..0x0009
62	0.495	Slave	LE LL	0	150µs	0	False	22	Empty PDU
63	0.517	Master	LE LL	0	22227µs	1	False	23	Empty PDU
64	0.517	Slave	ATT	10	150µs	1	True	23	Rcvd Find Information Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
65	0.517	Master	LE LL	0	150µs	0	False	23	Empty PDU
66	0.518	Slave	LE LL	0	150µs	0	False	23	Empty PDU
67	0.540	Master	ATT	9	21833µs	1	False	24	Sent Write Request, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
68	0.540	Slave	LE LL	0	150µs	1	False	24	Empty PDU
69	0.562	Master	LE LL	0	22227µs	0	False	25	Empty PDU
70	0.562	Slave	ATT	5	149µs	0	True	25	Rcvd Write Response, Handle: 0x0009 (Generic Attribute Profile: Service Changed: Client Characteristic Configuration)
71	0.562	Master	LE LL	0	151µs	1	False	25	Empty PDU
72	0.563	Slave	LE LL	0	149µs	1	False	25	Empty PDU
73	0.585	Master	ATT	11	21856µs	0	False	26	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x000a..0xffff
74	0.585	Slave	LE LL	0	150µs	0	False	26	Empty PDU
75	0.607	Master	LE LL	0	22218µs	1	False	27	Empty PDU
76	0.607	Slave	LE LL	27	150µs	1	True	27	L2CAP Fragment Start
77	0.608	Master	LE LL	0	150µs	0	False	27	Empty PDU
78	0.608	Slave	LE LL	21	150µs	0	True	27	L2CAP Fragment
79	0.608	Master	LE LL	0	150µs	1	False	27	Empty PDU
80	0.608	Slave	LE LL	0	150µs	1	False	27	Empty PDU
81	0.630	Master	ATT	11	21294µs	0	False	28	Sent Read By Type Request, GATT Characteristic Declaration, Handles: 0x000f..0xffff

82	0.630	Slave	LE LL	0	150µs	0	False	28	Empty PDU
83	0.652	Master	LE LL	0	22219µs	1	False	29	Empty PDU
84	0.652	Slave	ATT	9	150µs	1	True	29	Rcvd Error Response - Attribute Not Found, Handle: 0x000f (ZigBee Alliance: Unknown)
85	0.652	Master	LE LL	0	150µs	0	False	29	Empty PDU
86	0.653	Slave	LE LL	0	150µs	0	False	29	Empty PDU
87	0.675	Master	ATT	16	21838µs	1	False	30	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
88	0.675	Slave	LE LL	0	150µs	1	False	30	Empty PDU
89	0.697	Master	LE LL	0	22199µs	0	False	31	Empty PDU
90	0.697	Slave	ATT	5	150µs	0	True	31	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
91	0.697	Master	LE LL	0	150µs	1	False	31	Empty PDU
92	0.698	Slave	LE LL	0	150µs	1	False	31	Empty PDU
93	0.720	Master	ATT	9	21855µs	0	False	32	Sent Find Information Request, Handles: 0x000f..0xffff
94	0.720	Slave	LE LL	0	150µs	0	False	32	Empty PDU
95	0.742	Master	LE LL	0	22226µs	1	False	33	Empty PDU
96	0.742	Slave	ATT	10	150µs	1	True	33	Rcvd Find Information Response, Handle: 0x000f (ZigBee Alliance: Unknown: Client Characteristic Configuration)
97	0.742	Master	LE LL	0	150µs	0	False	33	Empty PDU
98	0.743	Slave	LE LL	0	150µs	0	False	33	Empty PDU
99	0.765	Master	ATT	9	21833µs	1	False	34	Sent Find Information Request, Handles: 0x0010..0xffff
100	0.765	Slave	LE LL	0	151µs	1	False	34	Empty PDU
101	0.787	Master	LE LL	0	22227µs	0	False	35	Empty PDU
102	0.787	Slave	ATT	9	150µs	0	True	35	Rcvd Error Response - Attribute Not Found, Handle: 0x0010 (ZigBee Alliance: Unknown)
103	0.787	Master	LE LL	0	150µs	1	False	35	Empty PDU
104	0.788	Slave	LE LL	0	150µs	1	False	35	Empty PDU
105	0.810	Master	ATT	9	21838µs	0	False	36	Sent Write Request, Handle: 0x000f (ZigBee Alliance: Unknown: Client Characteristic Configuration)
106	0.810	Slave	LE LL	0	150µs	0	False	36	Empty PDU
107	0.832	Master	LE LL	0	22226µs	1	False	37	Empty PDU
108	0.832	Slave	ATT	5	150µs	1	True	37	Rcvd Write Response, Handle: 0x000f (ZigBee Alliance: Unknown: Client Characteristic Configuration)
109	0.832	Master	LE LL	0	150µs	0	False	37	Empty PDU
110	0.833	Slave	ATT	13	150µs	0	True	37	Rcvd Handle Value Indication, Handle: 0x000e (ZigBee Alliance: Unknown)
111	0.833	Master	LE LL	0	150µs	1	False	37	Empty PDU
112	0.833	Slave	LE LL	0	150µs	1	False	37	Empty PDU
113	0.855	Master	ATT	5	21414µs	0	True	38	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
114	0.855	Slave	LE LL	0	150µs	0	False	38	Empty PDU
115	0.855	Master	ATT	80	150µs	1	False	38	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
116	0.855	Slave	LE LL	0	150µs	1	False	38	Empty PDU
117	0.877	Master	LE LL	0	21535µs	0	False	39	Empty PDU
118	0.877	Slave	ATT	5	150µs	0	True	39	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
119	0.877	Master	LE LL	0	150µs	1	False	39	Empty PDU
120	0.878	Slave	LE LL	0	150µs	1	False	39	Empty PDU
121	0.900	Master	LE LL	0	21854µs	0	False	40	Empty PDU
122	0.900	Slave	LE LL	0	150µs	0	False	40	Empty PDU
123	0.922	Master	LE LL	0	22262µs	1	False	41	Empty PDU

124	0.922	Slave	LE LL	27	150µs	1	True	41	L2CAP Fragment Start
125	0.923	Master	LE LL	0	150µs	0	False	41	Empty PDU
126	0.923	Slave	LE LL	27	150µs	0	True	41	L2CAP Fragment
127	0.923	Master	LE LL	0	150µs	1	False	41	Empty PDU
128	0.923	Slave	LE LL	27	150µs	1	True	41	L2CAP Fragment
129	0.945	Master	LE LL	0	21163µs	0	False	42	Empty PDU
130	0.945	Slave	LE LL	27	149µs	0	True	42	L2CAP Fragment
131	0.945	Master	LE LL	0	151µs	1	False	42	Empty PDU
132	0.945	Slave	LE LL	27	149µs	1	True	42	L2CAP Fragment
133	0.946	Master	LE LL	0	151µs	0	False	42	Empty PDU
134	0.946	Slave	LE LL	1	150µs	0	True	42	L2CAP Fragment
135	0.946	Master	LE LL	0	150µs	1	False	42	Empty PDU
136	0.946	Slave	LE LL	0	150µs	1	False	42	Empty PDU
137	0.967	Master	ATT	5	20878µs	0	False	43	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
138	0.967	Slave	LE LL	0	150µs	0	False	43	Empty PDU
139	0.990	Master	LE LL	0	22242µs	1	False	44	Empty PDU
140	0.990	Slave	LE LL	0	150µs	1	False	44	Empty PDU
141	1.012	Master	LE LL	0	22261µs	0	False	45	Empty PDU
142	1.012	Slave	LE LL	0	150µs	0	False	45	Empty PDU
143	1.035	Master	LE LL	0	22262µs	1	False	46	Empty PDU
144	1.035	Slave	LE LL	0	150µs	1	False	46	Empty PDU
145	1.057	Master	LE LL	0	22263µs	0	False	47	Empty PDU
146	1.057	Slave	LE LL	0	150µs	0	False	47	Empty PDU
147	1.080	Master	ATT	104	22263µs	1	False	48	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
148	1.080	Slave	LE LL	0	150µs	1	False	48	Empty PDU
149	1.102	Master	LE LL	0	21846µs	0	False	49	Empty PDU
150	1.102	Slave	ATT	5	150µs	0	True	49	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
151	1.102	Master	LE LL	0	150µs	1	False	49	Empty PDU
152	1.103	Slave	LE LL	0	150µs	1	False	49	Empty PDU
153	1.125	Master	LE LL	0	21855µs	0	False	50	Empty PDU
154	1.125	Slave	LE LL	0	149µs	0	False	50	Empty PDU
155	1.147	Master	LE LL	0	22263µs	1	False	51	Empty PDU
156	1.147	Slave	LE LL	0	150µs	1	False	51	Empty PDU
157	1.170	Master	LE LL	0	22262µs	0	False	52	Empty PDU
158	1.170	Slave	LE LL	0	150µs	0	False	52	Empty PDU
159	1.192	Master	LE LL	0	22262µs	1	False	53	Empty PDU
160	1.192	Slave	LE LL	0	150µs	1	False	53	Empty PDU
161	1.215	Master	LE LL	0	22263µs	0	False	54	Empty PDU
162	1.215	Slave	LE LL	0	150µs	0	False	54	Empty PDU
163	1.237	Master	LE LL	0	22261µs	1	False	55	Empty PDU
164	1.237	Slave	LE LL	0	150µs	1	False	55	Empty PDU
165	1.260	Master	LE LL	0	22262µs	0	False	56	Empty PDU
166	1.260	Slave	LE LL	0	150µs	0	False	56	Empty PDU
167	1.282	Master	LE LL	0	22263µs	1	False	57	Empty PDU
168	1.282	Slave	LE LL	0	150µs	1	False	57	Empty PDU

169	1.305	Master	LE LL	0	22262µs	0	False	58	Empty PDU
170	1.305	Slave	LE LL	0	150µs	0	False	58	Empty PDU
171	1.327	Master	LE LL	0	22263µs	1	False	59	Empty PDU
172	1.327	Slave	LE LL	0	150µs	1	False	59	Empty PDU
173	1.350	Master	LE LL	0	22262µs	0	False	60	Empty PDU
174	1.350	Slave	LE LL	0	150µs	0	False	60	Empty PDU
175	1.372	Master	LE LL	0	22262µs	1	False	61	Empty PDU
176	1.372	Slave	LE LL	0	150µs	1	False	61	Empty PDU
177	1.395	Master	LE LL	0	22263µs	0	False	62	Empty PDU
178	1.395	Slave	LE LL	0	150µs	0	False	62	Empty PDU
179	1.417	Master	LE LL	0	22262µs	1	False	63	Empty PDU
180	1.417	Slave	LE LL	0	150µs	1	False	63	Empty PDU
181	1.440	Master	LE LL	0	22262µs	0	False	64	Empty PDU
182	1.440	Slave	LE LL	0	150µs	0	False	64	Empty PDU
183	1.462	Master	LE LL	0	22263µs	1	False	65	Empty PDU
184	1.462	Slave	LE LL	0	150µs	1	False	65	Empty PDU
185	1.485	Master	LE LL	0	22262µs	0	False	66	Empty PDU
186	1.485	Slave	LE LL	0	150µs	0	False	66	Empty PDU
187	1.507	Master	LE LL	0	22261µs	1	False	67	Empty PDU
188	1.507	Slave	LE LL	0	150µs	1	False	67	Empty PDU
189	1.530	Master	LE LL	0	22263µs	0	False	68	Empty PDU
190	1.530	Slave	LE LL	0	149µs	0	False	68	Empty PDU
191	1.552	Master	LE LL	0	22264µs	1	False	69	Empty PDU
192	1.552	Slave	LE LL	0	150µs	1	False	69	Empty PDU
193	1.575	Master	LE LL	0	22262µs	0	False	70	Empty PDU
194	1.575	Slave	LE LL	0	150µs	0	False	70	Empty PDU
195	1.597	Master	LE LL	0	22262µs	1	False	71	Empty PDU
196	1.597	Slave	LE LL	0	150µs	1	False	71	Empty PDU
197	1.620	Master	LE LL	0	22263µs	0	False	72	Empty PDU
198	1.620	Slave	LE LL	0	150µs	0	False	72	Empty PDU
199	1.642	Master	LE LL	0	22263µs	1	False	73	Empty PDU
200	1.642	Slave	LE LL	0	150µs	1	False	73	Empty PDU
201	1.665	Master	LE LL	0	22261µs	0	False	74	Empty PDU
202	1.665	Slave	LE LL	0	150µs	0	False	74	Empty PDU
203	1.687	Master	LE LL	0	22262µs	1	False	75	Empty PDU
204	1.687	Slave	LE LL	0	150µs	1	False	75	Empty PDU
205	1.710	Master	LE LL	0	22262µs	0	False	76	Empty PDU
206	1.710	Slave	LE LL	0	150µs	0	False	76	Empty PDU
207	1.732	Master	LE LL	0	22263µs	1	False	77	Empty PDU
208	1.732	Slave	LE LL	0	150µs	1	False	77	Empty PDU
209	1.755	Master	LE LL	0	22263µs	0	False	78	Empty PDU
210	1.755	Slave	LE LL	0	150µs	0	False	78	Empty PDU
211	1.777	Master	LE LL	0	22261µs	1	False	79	Empty PDU
212	1.777	Slave	LE LL	0	149µs	1	False	79	Empty PDU
213	1.800	Master	LE LL	0	22263µs	0	False	80	Empty PDU

214	1.800	Slave	LE LL	0	150µs	0	False	80	Empty PDU
215	1.822	Master	LE LL	0	22262µs	1	False	81	Empty PDU
216	1.822	Slave	LE LL	0	150µs	1	False	81	Empty PDU
217	1.845	Master	LE LL	0	22264µs	0	False	82	Empty PDU
218	1.845	Slave	LE LL	0	149µs	0	False	82	Empty PDU
219	1.867	Master	LE LL	0	22263µs	1	False	83	Empty PDU
220	1.867	Slave	LE LL	0	149µs	1	False	83	Empty PDU
221	1.890	Master	LE LL	0	22264µs	0	False	84	Empty PDU
222	1.890	Slave	LE LL	0	150µs	0	False	84	Empty PDU
223	1.912	Master	LE LL	0	22262µs	1	False	85	Empty PDU
224	1.912	Slave	LE LL	0	150µs	1	False	85	Empty PDU
225	1.935	Master	LE LL	0	22262µs	0	False	86	Empty PDU
226	1.935	Slave	LE LL	0	150µs	0	False	86	Empty PDU
227	1.957	Master	LE LL	0	22261µs	1	False	87	Empty PDU
228	1.957	Slave	LE LL	0	150µs	1	False	87	Empty PDU
229	1.980	Master	LE LL	0	22262µs	0	False	88	Empty PDU
230	1.980	Slave	LE LL	0	150µs	0	False	88	Empty PDU
231	2.002	Master	LE LL	0	22264µs	1	False	89	Empty PDU
232	2.002	Slave	LE LL	0	149µs	1	False	89	Empty PDU
233	2.025	Master	LE LL	0	22263µs	0	False	90	Empty PDU
234	2.025	Slave	LE LL	0	150µs	0	False	90	Empty PDU
235	2.047	Master	LE LL	0	22261µs	1	False	91	Empty PDU
236	2.047	Slave	LE LL	0	150µs	1	False	91	Empty PDU
237	2.070	Master	LE LL	0	22262µs	0	False	92	Empty PDU
238	2.070	Slave	LE LL	0	150µs	0	False	92	Empty PDU
239	2.092	Master	LE LL	0	22264µs	1	False	93	Empty PDU
240	2.092	Slave	LE LL	0	150µs	1	False	93	Empty PDU
241	2.115	Master	LE LL	0	22262µs	0	False	94	Empty PDU
242	2.115	Slave	LE LL	0	150µs	0	False	94	Empty PDU
243	2.137	Master	LE LL	0	22263µs	1	False	95	Empty PDU
244	2.137	Slave	LE LL	0	150µs	1	False	95	Empty PDU
245	2.160	Master	LE LL	0	22262µs	0	False	96	Empty PDU
246	2.160	Slave	LE LL	0	150µs	0	False	96	Empty PDU
247	2.182	Master	LE LL	0	22263µs	1	False	97	Empty PDU
248	2.182	Slave	LE LL	27	149µs	1	True	97	L2CAP Fragment Start
249	2.183	Master	LE LL	0	151µs	0	False	97	Empty PDU
250	2.183	Slave	LE LL	27	149µs	0	True	97	L2CAP Fragment
251	2.183	Master	LE LL	0	151µs	1	False	97	Empty PDU
252	2.183	Slave	LE LL	27	149µs	1	True	97	L2CAP Fragment
253	2.184	Master	LE LL	0	151µs	0	False	97	Empty PDU
254	2.184	Slave	LE LL	27	149µs	0	True	97	L2CAP Fragment
255	2.184	Master	LE LL	0	151µs	1	False	97	Empty PDU
256	2.184	Slave	LE LL	27	149µs	1	True	97	L2CAP Fragment
257	2.185	Master	LE LL	0	151µs	0	False	97	Empty PDU
258	2.185	Slave	LE LL	4	149µs	0	True	97	L2CAP Fragment

259	2.185	Master	LE LL	0	151µs	1	False	97	Empty PDU
260	2.185	Slave	LE LL	0	149µs	1	False	97	Empty PDU
261	2.205	Master	ATT	5	19378µs	0	False	98	Sent Handle Value Confirmation
262	2.205	Slave	LE LL	0	150µs	0	False	98	Empty PDU
263	2.227	Master	LE LL	0	22243µs	1	False	99	Empty PDU
264	2.227	Slave	LE LL	0	150µs	1	False	99	Empty PDU
265	2.250	Master	ATT	71	22263µs	0	False	100	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
266	2.250	Slave	LE LL	0	150µs	0	False	100	Empty PDU
267	2.272	Master	LE LL	0	21978µs	1	False	101	Empty PDU
268	2.272	Slave	ATT	5	150µs	1	True	101	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
269	2.272	Master	LE LL	0	150µs	0	False	101	Empty PDU
270	2.273	Slave	LE LL	0	150µs	0	False	101	Empty PDU
271	2.295	Master	LE LL	0	21853µs	1	False	102	Empty PDU
272	2.295	Slave	LE LL	0	151µs	1	False	102	Empty PDU
273	2.317	Master	LE LL	0	22262µs	0	False	103	Empty PDU
274	2.317	Slave	LE LL	27	150µs	0	True	103	L2CAP Fragment Start
275	2.318	Master	LE LL	0	150µs	1	False	103	Empty PDU
276	2.318	Slave	LE LL	15	150µs	1	True	103	L2CAP Fragment
277	2.318	Master	LE LL	0	150µs	0	False	103	Empty PDU
278	2.318	Slave	LE LL	0	150µs	0	False	103	Empty PDU
279	2.340	Master	ATT	5	21319µs	1	True	104	Sent Handle Value Confirmation
280	2.340	Slave	LE LL	0	150µs	1	False	104	Empty PDU
281	2.340	Master	ATT	63	150µs	0	False	104	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
282	2.340	Slave	LE LL	0	150µs	0	False	104	Empty PDU
283	2.362	Master	LE LL	0	21602µs	1	False	105	Empty PDU
284	2.362	Slave	ATT	5	150µs	1	True	105	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
285	2.362	Master	LE LL	0	150µs	0	False	105	Empty PDU
286	2.363	Slave	LE LL	0	150µs	0	False	105	Empty PDU
287	2.385	Master	LE LL	0	21854µs	1	False	106	Empty PDU
288	2.385	Slave	LE LL	0	150µs	1	False	106	Empty PDU
289	2.407	Master	LE LL	0	22264µs	0	False	107	Empty PDU
290	2.407	Slave	LE LL	27	149µs	0	True	107	L2CAP Fragment Start
291	2.408	Master	LE LL	0	151µs	1	False	107	Empty PDU
292	2.408	Slave	LE LL	27	149µs	1	True	107	L2CAP Fragment
293	2.408	Master	LE LL	0	151µs	0	False	107	Empty PDU
294	2.408	Slave	LE LL	26	149µs	0	True	107	L2CAP Fragment
295	2.452	Master	ATT	63	43667µs	1	False	109	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
296	2.452	Slave	LE LL	0	150µs	1	False	109	Empty PDU
297	2.475	Master	LE LL	0	22010µs	0	False	110	Empty PDU
298	2.475	Slave	ATT	5	151µs	0	True	110	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
299	2.475	Master	LE LL	0	149µs	1	False	110	Empty PDU
300	2.475	Slave	LE LL	0	151µs	1	False	110	Empty PDU
301	2.497	Master	LE LL	0	21853µs	0	False	111	Empty PDU
302	2.497	Slave	LE LL	0	149µs	0	False	111	Empty PDU
303	2.520	Master	LE LL	0	22263µs	1	False	112	Empty PDU

304	2.520	Slave	LE LL	27	150µs	1	True	112	L2CAP Fragment Start
305	2.520	Master	LE LL	0	150µs	0	False	112	Empty PDU
306	2.520	Slave	LE LL	27	150µs	0	True	112	L2CAP Fragment
307	2.521	Master	LE LL	0	150µs	1	False	112	Empty PDU
308	2.521	Slave	LE LL	27	150µs	1	True	112	L2CAP Fragment
309	2.521	Master	LE LL	0	150µs	0	False	112	Empty PDU
310	2.521	Slave	LE LL	27	150µs	0	True	112	L2CAP Fragment
311	2.522	Master	LE LL	0	150µs	1	False	112	Empty PDU
312	2.522	Slave	LE LL	12	150µs	1	True	112	L2CAP Fragment
313	2.522	Master	LE LL	0	150µs	0	False	112	Empty PDU
314	2.522	Slave	LE LL	0	150µs	0	False	112	Empty PDU
315	2.542	Master	ATT	5	19843µs	1	True	113	Sent Handle Value Confirmation
316	2.542	Slave	LE LL	0	150µs	1	False	113	Empty PDU
317	2.542	Master	ATT	64	151µs	0	False	113	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
318	2.543	Slave	LE LL	0	149µs	0	False	113	Empty PDU
319	2.565	Master	LE LL	0	21598µs	1	False	114	Empty PDU
320	2.565	Slave	ATT	5	150µs	1	True	114	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
321	2.565	Master	LE LL	0	150µs	0	False	114	Empty PDU
322	2.565	Slave	LE LL	0	150µs	0	False	114	Empty PDU
323	2.587	Master	LE LL	0	21854µs	1	False	115	Empty PDU
324	2.587	Slave	LE LL	0	150µs	1	False	115	Empty PDU
325	2.610	Master	LE LL	0	22262µs	0	False	116	Empty PDU
326	2.610	Slave	LE LL	27	150µs	0	True	116	L2CAP Fragment Start
327	2.610	Master	LE LL	0	150µs	1	False	116	Empty PDU
328	2.610	Slave	LE LL	27	150µs	1	True	116	L2CAP Fragment
329	2.611	Master	LE LL	0	150µs	0	False	116	Empty PDU
330	2.611	Slave	LE LL	25	150µs	0	True	116	L2CAP Fragment
331	2.611	Master	LE LL	0	150µs	1	False	116	Empty PDU
332	2.611	Slave	LE LL	0	150µs	1	False	116	Empty PDU
333	2.632	Master	ATT	5	20783µs	0	False	117	Sent Handle Value Confirmation
334	2.632	Slave	LE LL	0	150µs	0	False	117	Empty PDU
335	2.655	Master	ATT	63	22241µs	1	False	118	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
336	2.655	Slave	LE LL	0	150µs	1	False	118	Empty PDU
337	2.677	Master	LE LL	0	22010µs	0	False	119	Empty PDU
338	2.677	Slave	ATT	5	150µs	0	True	119	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
339	2.677	Master	LE LL	0	150µs	1	False	119	Empty PDU
340	2.678	Slave	LE LL	0	150µs	1	False	119	Empty PDU
341	2.700	Master	LE LL	0	21856µs	0	False	120	Empty PDU
342	2.700	Slave	LE LL	0	150µs	0	False	120	Empty PDU
343	2.722	Master	LE LL	0	22261µs	1	False	121	Empty PDU
344	2.722	Slave	LE LL	27	150µs	1	True	121	L2CAP Fragment Start
345	2.723	Master	LE LL	0	150µs	0	False	121	Empty PDU
346	2.723	Slave	LE LL	27	150µs	0	True	121	L2CAP Fragment
347	2.723	Master	LE LL	0	150µs	1	False	121	Empty PDU
348	2.723	Slave	LE LL	26	150µs	1	True	121	L2CAP Fragment

349	2.745	Master	LE LL	0	21166µs	0	True	122	Empty PDU
350	2.745	Slave	LE LL	0	150µs	0	False	122	Empty PDU
351	2.745	Master	ATT	5	150µs	1	True	122	Sent Handle Value Confirmation
352	2.745	Slave	LE LL	0	150µs	1	False	122	Empty PDU
353	2.745	Master	ATT	63	150µs	0	False	122	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
354	2.746	Slave	LE LL	0	150µs	0	False	122	Empty PDU
355	2.767	Master	LE LL	0	21214µs	1	False	123	Empty PDU
356	2.767	Slave	ATT	5	150µs	1	True	123	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
357	2.767	Master	LE LL	0	150µs	0	False	123	Empty PDU
358	2.768	Slave	LE LL	0	150µs	0	False	123	Empty PDU
359	2.790	Master	LE LL	0	21856µs	1	False	124	Empty PDU
360	2.790	Slave	LE LL	0	149µs	1	False	124	Empty PDU
361	2.812	Master	LE LL	0	22263µs	0	False	125	Empty PDU
362	2.812	Slave	LE LL	27	150µs	0	True	125	L2CAP Fragment Start
363	2.813	Master	LE LL	0	150µs	1	False	125	Empty PDU
364	2.813	Slave	LE LL	27	150µs	1	True	125	L2CAP Fragment
365	2.813	Master	LE LL	0	150µs	0	False	125	Empty PDU
366	2.813	Slave	LE LL	27	150µs	0	True	125	L2CAP Fragment
367	2.814	Master	LE LL	0	150µs	1	False	125	Empty PDU
368	2.814	Slave	LE LL	27	150µs	1	True	125	L2CAP Fragment
369	2.814	Master	LE LL	0	150µs	0	False	125	Empty PDU
370	2.814	Slave	LE LL	12	150µs	0	True	125	L2CAP Fragment
371	2.814	Master	LE LL	0	150µs	1	False	125	Empty PDU
372	2.815	Slave	LE LL	0	150µs	1	False	125	Empty PDU
373	2.835	Master	ATT	5	19841µs	0	True	126	Sent Handle Value Confirmation
374	2.835	Slave	LE LL	0	150µs	0	False	126	Empty PDU
375	2.835	Master	ATT	63	150µs	1	False	126	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
376	2.835	Slave	LE LL	0	150µs	1	False	126	Empty PDU
377	2.857	Master	LE LL	0	21602µs	0	False	127	Empty PDU
378	2.857	Slave	ATT	5	150µs	0	True	127	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
379	2.857	Master	LE LL	0	150µs	1	False	127	Empty PDU
380	2.858	Slave	LE LL	0	150µs	1	False	127	Empty PDU
381	2.880	Master	LE LL	0	21854µs	0	False	128	Empty PDU
382	2.880	Slave	LE LL	0	150µs	0	False	128	Empty PDU
383	2.902	Master	LE LL	0	22264µs	1	False	129	Empty PDU
384	2.902	Slave	LE LL	27	150µs	1	True	129	L2CAP Fragment Start
385	2.903	Master	LE LL	0	150µs	0	False	129	Empty PDU
386	2.903	Slave	LE LL	27	150µs	0	True	129	L2CAP Fragment
387	2.903	Master	LE LL	0	150µs	1	False	129	Empty PDU
388	2.903	Slave	LE LL	24	150µs	1	True	129	L2CAP Fragment
389	2.904	Master	LE LL	0	150µs	0	False	129	Empty PDU
390	2.904	Slave	LE LL	0	150µs	0	False	129	Empty PDU
391	2.925	Master	ATT	5	20785µs	1	True	130	Sent Handle Value Confirmation
392	2.925	Slave	LE LL	0	150µs	1	False	130	Empty PDU
393	2.925	Master	ATT	64	150µs	0	False	130	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)

394	2.925	Slave	LE LL	0	150µs	0	False	130	Empty PDU
395	2.947	Master	LE LL	0	21599µs	1	False	131	Empty PDU
396	2.947	Slave	ATT	5	151µs	1	True	131	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
397	2.947	Master	LE LL	0	149µs	0	False	131	Empty PDU
398	2.948	Slave	LE LL	0	150µs	0	False	131	Empty PDU
399	2.970	Master	LE LL	0	21855µs	1	False	132	Empty PDU
400	2.970	Slave	LE LL	0	150µs	1	False	132	Empty PDU
401	2.992	Master	LE LL	0	22262µs	0	False	133	Empty PDU
402	2.992	Slave	LE LL	27	150µs	0	True	133	L2CAP Fragment Start
403	2.993	Master	LE LL	0	150µs	1	False	133	Empty PDU
404	2.993	Slave	LE LL	27	150µs	1	True	133	L2CAP Fragment
405	2.993	Master	LE LL	0	150µs	0	False	133	Empty PDU
406	2.993	Slave	LE LL	25	150µs	0	True	133	L2CAP Fragment
407	2.994	Master	LE LL	0	150µs	1	False	133	Empty PDU
408	2.994	Slave	LE LL	0	150µs	1	False	133	Empty PDU
409	3.015	Master	ATT	5	20783µs	0	False	134	Sent Handle Value Confirmation
410	3.015	Slave	LE LL	0	149µs	0	False	134	Empty PDU
411	3.037	Master	ATT	135	22242µs	1	False	135	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
412	3.038	Slave	LE LL	0	150µs	1	False	135	Empty PDU
413	3.060	Master	LE LL	0	21723µs	0	False	136	Empty PDU
414	3.060	Slave	ATT	5	150µs	0	True	136	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
415	3.060	Master	LE LL	0	150µs	1	False	136	Empty PDU
416	3.060	Slave	LE LL	0	150µs	1	False	136	Empty PDU
417	3.082	Master	LE LL	0	21854µs	0	False	137	Empty PDU
418	3.082	Slave	LE LL	0	151µs	0	False	137	Empty PDU
419	3.105	Master	LE LL	0	22262µs	1	False	138	Empty PDU
420	3.105	Slave	LE LL	27	149µs	1	True	138	L2CAP Fragment Start
421	3.105	Master	LE LL	0	151µs	0	False	138	Empty PDU
422	3.105	Slave	LE LL	27	149µs	0	True	138	L2CAP Fragment
423	3.106	Master	LE LL	0	151µs	1	False	138	Empty PDU
424	3.106	Slave	LE LL	27	149µs	1	True	138	L2CAP Fragment
425	3.106	Master	LE LL	0	151µs	0	False	138	Empty PDU
426	3.106	Slave	LE LL	27	149µs	0	True	138	L2CAP Fragment
427	3.107	Master	LE LL	0	151µs	1	False	138	Empty PDU
428	3.107	Slave	LE LL	27	149µs	1	True	138	L2CAP Fragment
429	3.107	Master	LE LL	0	151µs	0	False	138	Empty PDU
430	3.107	Slave	LE LL	27	149µs	0	True	138	L2CAP Fragment
431	3.108	Master	LE LL	0	151µs	1	False	138	Empty PDU
432	3.108	Slave	LE LL	27	149µs	1	True	138	L2CAP Fragment
433	3.108	Master	LE LL	0	151µs	0	False	138	Empty PDU
434	3.108	Slave	LE LL	27	149µs	0	True	138	L2CAP Fragment
435	3.109	Master	LE LL	0	151µs	1	False	138	Empty PDU
436	3.109	Slave	LE LL	27	149µs	1	True	138	L2CAP Fragment
437	3.109	Master	LE LL	0	151µs	0	False	138	Empty PDU
438	3.109	Slave	LE LL	8	149µs	0	True	138	L2CAP Fragment

439	3.109	Master	LE LL	0	151µs	1	False	138	Empty PDU
440	3.110	Slave	LE LL	0	149µs	1	False	138	Empty PDU
441	3.127	Master	ATT	5	17379µs	0	False	139	Sent Handle Value Confirmation
442	3.127	Slave	LE LL	0	150µs	0	False	139	Empty PDU
443	3.150	Master	LE LL	0	22242µs	1	False	140	Empty PDU
444	3.150	Slave	LE LL	27	150µs	1	True	140	L2CAP Fragment Start
445	3.150	Master	LE LL	0	150µs	0	False	140	Empty PDU
446	3.150	Slave	LE LL	1	150µs	0	True	140	L2CAP Fragment
447	3.150	Master	LE LL	0	150µs	1	False	140	Empty PDU
448	3.151	Slave	LE LL	0	150µs	1	False	140	Empty PDU
449	3.172	Master	ATT	5	21373µs	0	True	141	Sent Handle Value Confirmation
450	3.172	Slave	LE LL	0	151µs	0	False	141	Empty PDU
451	3.172	Master	ATT	77	149µs	1	False	141	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
452	3.173	Slave	LE LL	0	151µs	1	False	141	Empty PDU
453	3.195	Master	LE LL	0	21546µs	0	False	142	Empty PDU
454	3.195	Slave	ATT	5	149µs	0	True	142	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
455	3.195	Master	LE LL	0	151µs	1	False	142	Empty PDU
456	3.195	Slave	LE LL	0	149µs	1	False	142	Empty PDU
457	3.217	Master	LE LL	0	21855µs	0	False	143	Empty PDU
458	3.217	Slave	LE LL	0	150µs	0	False	143	Empty PDU
459	3.240	Master	LE LL	0	22262µs	1	False	144	Empty PDU
460	3.240	Slave	LE LL	0	150µs	1	False	144	Empty PDU
461	3.262	Master	LE LL	0	22262µs	0	False	145	Empty PDU
462	3.262	Slave	LE LL	27	150µs	0	True	145	L2CAP Fragment Start
463	3.263	Master	LE LL	0	150µs	1	False	145	Empty PDU
464	3.263	Slave	LE LL	27	150µs	1	True	145	L2CAP Fragment
465	3.263	Master	LE LL	0	150µs	0	False	145	Empty PDU
466	3.263	Slave	LE LL	24	150µs	0	True	145	L2CAP Fragment
467	3.264	Master	LE LL	0	150µs	1	False	145	Empty PDU
468	3.264	Slave	LE LL	0	150µs	1	False	145	Empty PDU
469	3.285	Master	ATT	5	20786µs	0	True	146	Sent Handle Value Confirmation
470	3.285	Slave	LE LL	0	150µs	0	False	146	Empty PDU
471	3.285	Master	ATT	82	150µs	1	False	146	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
472	3.285	Slave	LE LL	0	150µs	1	False	146	Empty PDU
473	3.307	Master	LE LL	0	21526µs	0	False	147	Empty PDU
474	3.307	Slave	ATT	5	150µs	0	True	147	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
475	3.307	Master	LE LL	0	150µs	1	False	147	Empty PDU
476	3.308	Slave	LE LL	0	150µs	1	False	147	Empty PDU
477	3.330	Master	LE LL	0	21854µs	0	False	148	Empty PDU
478	3.330	Slave	LE LL	0	150µs	0	False	148	Empty PDU
479	3.352	Master	LE LL	0	22263µs	1	False	149	Empty PDU
480	3.352	Slave	LE LL	0	150µs	1	False	149	Empty PDU
481	3.375	Master	LE LL	0	22262µs	0	False	150	Empty PDU
482	3.375	Slave	LE LL	0	150µs	0	False	150	Empty PDU
483	3.397	Master	LE LL	0	22262µs	1	False	151	Empty PDU

484	3.397	Slave	LE LL	27	150µs	1	True	151	L2CAP Fragment Start
485	3.398	Master	LE LL	0	150µs	0	False	151	Empty PDU
486	3.398	Slave	LE LL	27	150µs	0	True	151	L2CAP Fragment
487	3.398	Master	LE LL	0	150µs	1	False	151	Empty PDU
488	3.398	Slave	LE LL	24	150µs	1	True	151	L2CAP Fragment
489	3.399	Master	LE LL	0	150µs	0	False	151	Empty PDU
490	3.399	Slave	LE LL	0	150µs	0	False	151	Empty PDU
491	3.420	Master	ATT	5	20786µs	1	True	152	Sent Handle Value Confirmation
492	3.420	Slave	LE LL	0	150µs	1	False	152	Empty PDU
493	3.420	Master	ATT	74	150µs	0	False	152	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
494	3.420	Slave	LE LL	0	150µs	0	False	152	Empty PDU
495	3.442	Master	LE LL	0	21559µs	1	False	153	Empty PDU
496	3.442	Slave	ATT	5	150µs	1	True	153	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
497	3.442	Master	LE LL	0	150µs	0	False	153	Empty PDU
498	3.443	Slave	LE LL	0	150µs	0	False	153	Empty PDU
499	3.487	Master	LE LL	0	44355µs	1	False	155	Empty PDU
500	3.487	Slave	LE LL	27	150µs	1	True	155	L2CAP Fragment Start
501	3.488	Master	LE LL	0	150µs	0	False	155	Empty PDU
502	3.488	Slave	LE LL	27	150µs	0	True	155	L2CAP Fragment
503	3.488	Master	LE LL	0	150µs	1	False	155	Empty PDU
504	3.488	Slave	LE LL	27	150µs	1	True	155	L2CAP Fragment
505	3.489	Master	LE LL	0	150µs	0	False	155	Empty PDU
506	3.489	Slave	LE LL	27	150µs	0	True	155	L2CAP Fragment
507	3.489	Master	LE LL	0	150µs	1	False	155	Empty PDU
508	3.489	Slave	LE LL	27	150µs	1	True	155	L2CAP Fragment
509	3.490	Master	LE LL	0	150µs	0	False	155	Empty PDU
510	3.490	Slave	LE LL	27	150µs	0	True	155	L2CAP Fragment
511	3.490	Master	LE LL	0	150µs	1	False	155	Empty PDU
512	3.490	Slave	LE LL	27	150µs	1	True	155	L2CAP Fragment
513	3.491	Master	LE LL	0	150µs	0	False	155	Empty PDU
514	3.491	Slave	LE LL	27	150µs	0	True	155	L2CAP Fragment
515	3.491	Master	LE LL	0	150µs	1	False	155	Empty PDU
516	3.491	Slave	LE LL	27	150µs	1	True	155	L2CAP Fragment
517	3.492	Master	LE LL	0	150µs	0	False	155	Empty PDU
518	3.492	Slave	LE LL	8	150µs	0	True	155	L2CAP Fragment
519	3.492	Master	LE LL	0	150µs	1	False	155	Empty PDU
520	3.492	Slave	LE LL	0	150µs	1	False	155	Empty PDU
521	3.510	Master	ATT	5	17377µs	0	False	156	Sent Handle Value Confirmation
522	3.510	Slave	LE LL	0	150µs	0	False	156	Empty PDU
523	3.532	Master	LE LL	0	22242µs	1	False	157	Empty PDU
524	3.532	Slave	LE LL	27	150µs	1	True	157	L2CAP Fragment Start
525	3.533	Master	LE LL	0	150µs	0	False	157	Empty PDU
526	3.533	Slave	LE LL	27	150µs	0	True	157	L2CAP Fragment
527	3.533	Master	LE LL	0	150µs	1	False	157	Empty PDU
528	3.533	Slave	LE LL	27	150µs	1	True	157	L2CAP Fragment

529	3.534	Master	LE LL	0	150µs	0	False	157	Empty PDU
530	3.534	Slave	LE LL	27	150µs	0	True	157	L2CAP Fragment
531	3.534	Master	LE LL	0	150µs	1	False	157	Empty PDU
532	3.534	Slave	LE LL	27	150µs	1	True	157	L2CAP Fragment
533	3.535	Master	LE LL	0	150µs	0	False	157	Empty PDU
534	3.535	Slave	LE LL	27	150µs	0	True	157	L2CAP Fragment
535	3.535	Master	LE LL	0	150µs	1	False	157	Empty PDU
536	3.535	Slave	LE LL	27	150µs	1	True	157	L2CAP Fragment
537	3.536	Master	LE LL	0	150µs	0	False	157	Empty PDU
538	3.536	Slave	LE LL	27	150µs	0	True	157	L2CAP Fragment
539	3.536	Master	LE LL	0	150µs	1	False	157	Empty PDU
540	3.536	Slave	LE LL	27	150µs	1	True	157	L2CAP Fragment
541	3.537	Master	LE LL	0	150µs	0	False	157	Empty PDU
542	3.537	Slave	LE LL	8	150µs	0	True	157	L2CAP Fragment
543	3.537	Master	LE LL	0	150µs	1	False	157	Empty PDU
544	3.537	Slave	LE LL	0	150µs	1	False	157	Empty PDU
545	3.555	Master	ATT	5	17379µs	0	False	158	Sent Handle Value Confirmation
546	3.555	Slave	LE LL	0	150µs	0	False	158	Empty PDU
547	3.577	Master	LE LL	0	22241µs	1	False	159	Empty PDU
548	3.577	Slave	LE LL	27	151µs	1	True	159	L2CAP Fragment Start
549	3.578	Master	LE LL	0	149µs	0	False	159	Empty PDU
550	3.578	Slave	LE LL	27	150µs	0	True	159	L2CAP Fragment
551	3.578	Master	LE LL	0	150µs	1	False	159	Empty PDU
552	3.578	Slave	LE LL	1	151µs	1	True	159	L2CAP Fragment
553	3.578	Master	LE LL	0	149µs	0	False	159	Empty PDU
554	3.579	Slave	LE LL	0	151µs	0	False	159	Empty PDU
555	3.600	Master	ATT	5	20878µs	1	True	160	Sent Handle Value Confirmation
556	3.600	Slave	LE LL	0	150µs	1	False	160	Empty PDU
557	3.600	Master	ATT	74	150µs	0	False	160	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
558	3.600	Slave	LE LL	0	150µs	0	False	160	Empty PDU
559	3.622	Master	LE LL	0	21559µs	1	False	161	Empty PDU
560	3.622	Slave	ATT	5	150µs	1	True	161	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
561	3.622	Master	LE LL	0	150µs	0	False	161	Empty PDU
562	3.623	Slave	LE LL	0	150µs	0	False	161	Empty PDU
563	3.645	Master	LE LL	0	21854µs	1	False	162	Empty PDU
564	3.645	Slave	LE LL	0	150µs	1	False	162	Empty PDU
565	3.667	Master	LE LL	0	22262µs	0	False	163	Empty PDU
566	3.667	Slave	LE LL	27	151µs	0	True	163	L2CAP Fragment Start
567	3.668	Master	LE LL	0	149µs	1	False	163	Empty PDU
568	3.668	Slave	LE LL	27	151µs	1	True	163	L2CAP Fragment
569	3.668	Master	LE LL	0	150µs	0	False	163	Empty PDU
570	3.668	Slave	LE LL	27	150µs	0	True	163	L2CAP Fragment
571	3.669	Master	LE LL	0	150µs	1	False	163	Empty PDU
572	3.669	Slave	LE LL	27	150µs	1	True	163	L2CAP Fragment
573	3.669	Master	LE LL	0	150µs	0	False	163	Empty PDU

574	3.669	Slave	LE LL	27	150µs	0	True	163	L2CAP Fragment
575	3.670	Master	LE LL	0	150µs	1	False	163	Empty PDU
576	3.670	Slave	LE LL	27	150µs	1	True	163	L2CAP Fragment
577	3.670	Master	LE LL	0	150µs	0	False	163	Empty PDU
578	3.670	Slave	LE LL	27	150µs	0	True	163	L2CAP Fragment
579	3.671	Master	LE LL	0	150µs	1	False	163	Empty PDU
580	3.671	Slave	LE LL	27	150µs	1	True	163	L2CAP Fragment
581	3.671	Master	LE LL	0	150µs	0	False	163	Empty PDU
582	3.671	Slave	LE LL	27	150µs	0	True	163	L2CAP Fragment
583	3.672	Master	LE LL	0	150µs	1	False	163	Empty PDU
584	3.672	Slave	LE LL	8	150µs	1	True	163	L2CAP Fragment
585	3.672	Master	LE LL	0	150µs	0	False	163	Empty PDU
586	3.672	Slave	LE LL	0	150µs	0	False	163	Empty PDU
587	3.690	Master	ATT	5	17377µs	1	False	164	Sent Handle Value Confirmation
588	3.690	Slave	LE LL	0	150µs	1	False	164	Empty PDU
589	3.712	Master	LE LL	0	22243µs	0	False	165	Empty PDU
590	3.712	Slave	LE LL	27	149µs	0	True	165	L2CAP Fragment Start
591	3.713	Master	LE LL	0	151µs	1	False	165	Empty PDU
592	3.713	Slave	LE LL	27	149µs	1	True	165	L2CAP Fragment
593	3.713	Master	LE LL	0	151µs	0	False	165	Empty PDU
594	3.713	Slave	LE LL	27	149µs	0	True	165	L2CAP Fragment
595	3.714	Master	LE LL	0	151µs	1	False	165	Empty PDU
596	3.714	Slave	LE LL	27	150µs	1	True	165	L2CAP Fragment
597	3.714	Master	LE LL	0	150µs	0	False	165	Empty PDU
598	3.714	Slave	LE LL	27	150µs	0	True	165	L2CAP Fragment
599	3.715	Master	LE LL	0	150µs	1	False	165	Empty PDU
600	3.715	Slave	LE LL	27	150µs	1	True	165	L2CAP Fragment
601	3.715	Master	LE LL	0	150µs	0	False	165	Empty PDU
602	3.715	Slave	LE LL	27	150µs	0	True	165	L2CAP Fragment
603	3.716	Master	LE LL	0	150µs	1	False	165	Empty PDU
604	3.716	Slave	LE LL	27	150µs	1	True	165	L2CAP Fragment
605	3.716	Master	LE LL	0	150µs	0	False	165	Empty PDU
606	3.716	Slave	LE LL	27	150µs	0	True	165	L2CAP Fragment
607	3.717	Master	LE LL	0	150µs	1	False	165	Empty PDU
608	3.717	Slave	LE LL	8	150µs	1	True	165	L2CAP Fragment
609	3.717	Master	LE LL	0	150µs	0	False	165	Empty PDU
610	3.717	Slave	LE LL	0	150µs	0	False	165	Empty PDU
611	3.735	Master	ATT	5	17377µs	1	False	166	Sent Handle Value Confirmation
612	3.735	Slave	LE LL	0	150µs	1	False	166	Empty PDU
613	3.757	Master	LE LL	0	22243µs	0	False	167	Empty PDU
614	3.757	Slave	LE LL	27	150µs	0	True	167	L2CAP Fragment Start
615	3.758	Master	LE LL	0	150µs	1	False	167	Empty PDU
616	3.758	Slave	LE LL	27	150µs	1	True	167	L2CAP Fragment
617	3.758	Master	LE LL	0	150µs	0	False	167	Empty PDU
618	3.758	Slave	LE LL	27	150µs	0	True	167	L2CAP Fragment

619	3.759	Master	LE LL	0	150µs	1	False	167	Empty PDU
620	3.759	Slave	LE LL	4	150µs	1	True	167	L2CAP Fragment
621	3.759	Master	LE LL	0	150µs	0	False	167	Empty PDU
622	3.759	Slave	LE LL	0	150µs	0	False	167	Empty PDU
623	3.780	Master	ATT	5	20369µs	1	True	168	Sent Handle Value Confirmation
624	3.780	Slave	LE LL	0	150µs	1	False	168	Empty PDU
625	3.780	Master	ATT	106	150µs	0	False	168	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
626	3.781	Slave	LE LL	0	150µs	0	False	168	Empty PDU
627	3.802	Master	LE LL	0	21432µs	1	False	169	Empty PDU
628	3.802	Slave	ATT	5	149µs	1	True	169	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
629	3.802	Master	LE LL	0	151µs	0	False	169	Empty PDU
630	3.803	Slave	LE LL	0	149µs	0	False	169	Empty PDU
631	3.825	Master	LE LL	0	21855µs	1	False	170	Empty PDU
632	3.825	Slave	LE LL	0	150µs	1	False	170	Empty PDU
633	3.847	Master	LE LL	0	22262µs	0	False	171	Empty PDU
634	3.847	Slave	LE LL	0	150µs	0	False	171	Empty PDU
635	3.870	Master	LE LL	0	22263µs	1	False	172	Empty PDU
636	3.870	Slave	LE LL	0	150µs	1	False	172	Empty PDU
637	3.892	Master	LE LL	0	22262µs	0	False	173	Empty PDU
638	3.892	Slave	LE LL	0	150µs	0	False	173	Empty PDU
639	3.915	Master	LE LL	0	22262µs	1	False	174	Empty PDU
640	3.915	Slave	LE LL	0	150µs	1	False	174	Empty PDU
641	3.937	Master	LE LL	0	22262µs	0	False	175	Empty PDU
642	3.937	Slave	LE LL	0	150µs	0	False	175	Empty PDU
643	3.960	Master	LE LL	0	22262µs	1	False	176	Empty PDU
644	3.960	Slave	LE LL	0	150µs	1	False	176	Empty PDU
645	3.982	Master	LE LL	0	22263µs	0	False	177	Empty PDU
646	3.982	Slave	LE LL	0	150µs	0	False	177	Empty PDU
647	4.005	Master	LE LL	0	22262µs	1	False	178	Empty PDU
648	4.005	Slave	LE LL	0	150µs	1	False	178	Empty PDU
649	4.027	Master	LE LL	0	22262µs	0	False	179	Empty PDU
650	4.027	Slave	LE LL	0	150µs	0	False	179	Empty PDU
651	4.050	Master	LE LL	0	22262µs	1	False	180	Empty PDU
652	4.050	Slave	LE LL	0	150µs	1	False	180	Empty PDU
653	4.072	Master	LE LL	0	22263µs	0	False	181	Empty PDU
654	4.072	Slave	LE LL	27	150µs	0	True	181	L2CAP Fragment Start
655	4.073	Master	LE LL	0	150µs	1	False	181	Empty PDU
656	4.073	Slave	LE LL	27	150µs	1	True	181	L2CAP Fragment
657	4.073	Master	LE LL	0	150µs	0	False	181	Empty PDU
658	4.073	Slave	LE LL	27	150µs	0	True	181	L2CAP Fragment
659	4.074	Master	LE LL	0	150µs	1	False	181	Empty PDU
660	4.074	Slave	LE LL	27	150µs	1	True	181	L2CAP Fragment
661	4.074	Master	LE LL	0	150µs	0	False	181	Empty PDU
662	4.074	Slave	LE LL	27	150µs	0	True	181	L2CAP Fragment
663	4.075	Master	LE LL	0	150µs	1	False	181	Empty PDU

664	4.075	Slave	LE LL	27	150µs	1	True	181	L2CAP Fragment
665	4.075	Master	LE LL	0	150µs	0	False	181	Empty PDU
666	4.075	Slave	LE LL	27	150µs	0	True	181	L2CAP Fragment
667	4.076	Master	LE LL	0	150µs	1	False	181	Empty PDU
668	4.076	Slave	LE LL	27	150µs	1	True	181	L2CAP Fragment
669	4.076	Master	LE LL	0	150µs	0	False	181	Empty PDU
670	4.076	Slave	LE LL	27	150µs	0	True	181	L2CAP Fragment
671	4.077	Master	LE LL	0	150µs	1	False	181	Empty PDU
672	4.077	Slave	LE LL	8	150µs	1	True	181	L2CAP Fragment
673	4.077	Master	LE LL	0	150µs	0	False	181	Empty PDU
674	4.077	Slave	LE LL	0	150µs	0	False	181	Empty PDU
675	4.095	Master	ATT	5	17379µs	1	False	182	Sent Handle Value Confirmation
676	4.095	Slave	LE LL	0	150µs	1	False	182	Empty PDU
677	4.117	Master	LE LL	0	22242µs	0	False	183	Empty PDU
678	4.117	Slave	LE LL	27	150µs	0	True	183	L2CAP Fragment Start
679	4.118	Master	LE LL	0	150µs	1	False	183	Empty PDU
680	4.118	Slave	LE LL	27	150µs	1	True	183	L2CAP Fragment
681	4.118	Master	LE LL	0	150µs	0	False	183	Empty PDU
682	4.118	Slave	LE LL	27	150µs	0	True	183	L2CAP Fragment
683	4.119	Master	LE LL	0	150µs	1	False	183	Empty PDU
684	4.119	Slave	LE LL	27	150µs	1	True	183	L2CAP Fragment
685	4.119	Master	LE LL	0	150µs	0	False	183	Empty PDU
686	4.119	Slave	LE LL	27	150µs	0	True	183	L2CAP Fragment
687	4.120	Master	LE LL	0	150µs	1	False	183	Empty PDU
688	4.120	Slave	LE LL	27	150µs	1	True	183	L2CAP Fragment
689	4.120	Master	LE LL	0	150µs	0	False	183	Empty PDU
690	4.120	Slave	LE LL	27	150µs	0	True	183	L2CAP Fragment
691	4.121	Master	LE LL	0	150µs	1	False	183	Empty PDU
692	4.121	Slave	LE LL	27	150µs	1	True	183	L2CAP Fragment
693	4.121	Master	LE LL	0	150µs	0	False	183	Empty PDU
694	4.121	Slave	LE LL	27	150µs	0	True	183	L2CAP Fragment
695	4.122	Master	LE LL	0	150µs	1	False	183	Empty PDU
696	4.122	Slave	LE LL	8	150µs	1	True	183	L2CAP Fragment
697	4.122	Master	LE LL	0	150µs	0	False	183	Empty PDU
698	4.122	Slave	LE LL	0	150µs	0	False	183	Empty PDU
699	4.140	Master	ATT	5	17378µs	1	False	184	Sent Handle Value Confirmation
700	4.140	Slave	LE LL	0	150µs	1	False	184	Empty PDU
701	4.162	Master	LE LL	0	22242µs	0	False	185	Empty PDU
702	4.162	Slave	LE LL	27	150µs	0	True	185	L2CAP Fragment Start
703	4.163	Master	LE LL	0	150µs	1	False	185	Empty PDU
704	4.163	Slave	LE LL	27	150µs	1	True	185	L2CAP Fragment
705	4.163	Master	LE LL	0	150µs	0	False	185	Empty PDU
706	4.163	Slave	LE LL	27	150µs	0	True	185	L2CAP Fragment
707	4.164	Master	LE LL	0	150µs	1	False	185	Empty PDU
708	4.164	Slave	LE LL	27	150µs	1	True	185	L2CAP Fragment

709	4.164	Master	LE LL	0	150µs	0	False	185	Empty PDU
710	4.164	Slave	LE LL	27	150µs	0	True	185	L2CAP Fragment
711	4.165	Master	LE LL	0	150µs	1	False	185	Empty PDU
712	4.165	Slave	LE LL	27	150µs	1	True	185	L2CAP Fragment
713	4.165	Master	LE LL	0	150µs	0	False	185	Empty PDU
714	4.165	Slave	LE LL	27	150µs	0	True	185	L2CAP Fragment
715	4.166	Master	LE LL	0	150µs	1	False	185	Empty PDU
716	4.166	Slave	LE LL	27	150µs	1	True	185	L2CAP Fragment
717	4.166	Master	LE LL	0	150µs	0	False	185	Empty PDU
718	4.166	Slave	LE LL	26	150µs	0	True	185	L2CAP Fragment
719	4.167	Master	LE LL	0	150µs	1	False	185	Empty PDU
720	4.167	Slave	LE LL	0	150µs	1	False	185	Empty PDU
721	4.185	Master	ATT	5	17803µs	0	False	186	Sent Handle Value Confirmation
722	4.185	Slave	LE LL	0	150µs	0	False	186	Empty PDU
723	4.207	Master	LE LL	0	22241µs	1	False	187	Empty PDU
724	4.207	Slave	LE LL	0	150µs	1	False	187	Empty PDU
725	4.230	Master	ATT	77	22263µs	0	False	188	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
726	4.230	Slave	LE LL	0	150µs	0	False	188	Empty PDU
727	4.252	Master	LE LL	0	21954µs	1	False	189	Empty PDU
728	4.252	Slave	ATT	5	150µs	1	True	189	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
729	4.252	Master	LE LL	0	150µs	0	False	189	Empty PDU
730	4.253	Slave	LE LL	0	150µs	0	False	189	Empty PDU
731	4.275	Master	LE LL	0	21855µs	1	False	190	Empty PDU
732	4.275	Slave	LE LL	0	150µs	1	False	190	Empty PDU
733	4.297	Master	LE LL	0	22261µs	0	False	191	Empty PDU
734	4.297	Slave	LE LL	0	150µs	0	False	191	Empty PDU
735	4.320	Master	LE LL	0	22263µs	1	False	192	Empty PDU
736	4.320	Slave	LE LL	27	150µs	1	True	192	L2CAP Fragment Start
737	4.320	Master	LE LL	0	150µs	0	False	192	Empty PDU
738	4.320	Slave	LE LL	27	150µs	0	True	192	L2CAP Fragment
739	4.321	Master	LE LL	0	150µs	1	False	192	Empty PDU
740	4.321	Slave	LE LL	24	150µs	1	True	192	L2CAP Fragment
741	4.321	Master	LE LL	0	150µs	0	False	192	Empty PDU
742	4.321	Slave	LE LL	0	150µs	0	False	192	Empty PDU
743	4.342	Master	ATT	5	20785µs	1	False	193	Sent Handle Value Confirmation
744	4.342	Slave	LE LL	0	150µs	1	False	193	Empty PDU
745	4.365	Master	LE LL	0	22243µs	0	False	194	Empty PDU
746	4.365	Slave	LE LL	0	151µs	0	False	194	Empty PDU
747	4.387	Master	LE LL	0	22261µs	1	False	195	Empty PDU
748	4.387	Slave	LE LL	0	150µs	1	False	195	Empty PDU
749	4.410	Master	LE LL	0	22262µs	0	False	196	Empty PDU
750	4.410	Slave	LE LL	0	150µs	0	False	196	Empty PDU
751	4.432	Master	LE LL	0	22263µs	1	False	197	Empty PDU
752	4.432	Slave	LE LL	0	149µs	1	False	197	Empty PDU
753	4.455	Master	LE LL	0	22263µs	0	False	198	Empty PDU

754	4.455	Slave	LE LL	0	150µs	0	False	198	Empty PDU
755	4.477	Master	LE LL	0	22263µs	1	False	199	Empty PDU
756	4.477	Slave	LE LL	0	150µs	1	False	199	Empty PDU
757	4.500	Master	LE LL	0	22261µs	0	False	200	Empty PDU
758	4.500	Slave	LE LL	0	150µs	0	False	200	Empty PDU
759	4.522	Master	LE LL	0	22262µs	1	False	201	Empty PDU
760	4.522	Slave	LE LL	0	150µs	1	False	201	Empty PDU
761	4.545	Master	LE LL	0	22264µs	0	False	202	Empty PDU
762	4.545	Slave	LE LL	0	150µs	0	False	202	Empty PDU
763	4.567	Master	LE LL	0	22262µs	1	False	203	Empty PDU
764	4.567	Slave	LE LL	0	150µs	1	False	203	Empty PDU
765	4.590	Master	LE LL	0	22261µs	0	False	204	Empty PDU
766	4.590	Slave	LE LL	0	150µs	0	False	204	Empty PDU
767	4.612	Master	LE LL	0	22263µs	1	False	205	Empty PDU
768	4.612	Slave	LE LL	0	150µs	1	False	205	Empty PDU
769	4.635	Master	LE LL	0	22263µs	0	False	206	Empty PDU
770	4.635	Slave	LE LL	0	149µs	0	False	206	Empty PDU
771	4.657	Master	LE LL	0	22263µs	1	False	207	Empty PDU
772	4.657	Slave	LE LL	0	150µs	1	False	207	Empty PDU
773	4.680	Master	LE LL	0	22262µs	0	False	208	Empty PDU
774	4.680	Slave	LE LL	0	149µs	0	False	208	Empty PDU
775	4.702	Master	LE LL	0	22264µs	1	False	209	Empty PDU
776	4.702	Slave	LE LL	0	150µs	1	False	209	Empty PDU
777	4.725	Master	LE LL	0	22262µs	0	False	210	Empty PDU
778	4.725	Slave	LE LL	0	150µs	0	False	210	Empty PDU
779	4.747	Master	LE LL	0	22261µs	1	False	211	Empty PDU
780	4.747	Slave	LE LL	0	150µs	1	False	211	Empty PDU
781	4.770	Master	LE LL	0	22263µs	0	False	212	Empty PDU
782	4.770	Slave	LE LL	0	149µs	0	False	212	Empty PDU
783	4.792	Master	LE LL	0	22264µs	1	False	213	Empty PDU
784	4.792	Slave	LE LL	0	150µs	1	False	213	Empty PDU
785	4.815	Master	LE LL	0	22262µs	0	False	214	Empty PDU
786	4.815	Slave	LE LL	0	149µs	0	False	214	Empty PDU
787	4.837	Master	LE LL	0	22264µs	1	False	215	Empty PDU
788	4.837	Slave	LE LL	0	150µs	1	False	215	Empty PDU
789	4.860	Master	LE LL	0	22262µs	0	False	216	Empty PDU
790	4.860	Slave	LE LL	0	150µs	0	False	216	Empty PDU
791	4.882	Master	LE LL	0	22261µs	1	False	217	Empty PDU
792	4.882	Slave	LE LL	0	150µs	1	False	217	Empty PDU
793	4.905	Master	LE LL	0	22263µs	0	False	218	Empty PDU
794	4.905	Slave	LE LL	0	149µs	0	False	218	Empty PDU
795	4.927	Master	LE LL	0	22263µs	1	False	219	Empty PDU
796	4.927	Slave	LE LL	0	150µs	1	False	219	Empty PDU
797	4.950	Master	LE LL	0	22262µs	0	False	220	Empty PDU
798	4.950	Slave	LE LL	0	150µs	0	False	220	Empty PDU

799	4.972	Master	LE LL	0	22264µs	1	False	221	Empty PDU
800	4.972	Slave	LE LL	0	150µs	1	False	221	Empty PDU
801	4.995	Master	LE LL	0	22262µs	0	False	222	Empty PDU
802	4.995	Slave	LE LL	0	150µs	0	False	222	Empty PDU
803	5.017	Master	LE LL	0	22263µs	1	False	223	Empty PDU
804	5.017	Slave	LE LL	0	150µs	1	False	223	Empty PDU
805	5.040	Master	LE LL	0	22262µs	0	False	224	Empty PDU
806	5.040	Slave	LE LL	0	150µs	0	False	224	Empty PDU
807	5.062	Master	LE LL	0	22262µs	1	False	225	Empty PDU
808	5.062	Slave	LE LL	0	150µs	1	False	225	Empty PDU
809	5.085	Master	LE LL	0	22263µs	0	False	226	Empty PDU
810	5.085	Slave	LE LL	0	150µs	0	False	226	Empty PDU
811	5.107	Master	LE LL	0	22262µs	1	False	227	Empty PDU
812	5.107	Slave	LE LL	0	150µs	1	False	227	Empty PDU
813	5.130	Master	LE LL	0	22262µs	0	False	228	Empty PDU
814	5.130	Slave	LE LL	0	150µs	0	False	228	Empty PDU
815	5.152	Master	LE LL	0	22262µs	1	False	229	Empty PDU
816	5.152	Slave	LE LL	0	150µs	1	False	229	Empty PDU
817	5.175	Master	LE LL	0	22264µs	0	False	230	Empty PDU
818	5.175	Slave	LE LL	0	149µs	0	False	230	Empty PDU
819	5.197	Master	LE LL	0	22263µs	1	False	231	Empty PDU
820	5.197	Slave	LE LL	0	150µs	1	False	231	Empty PDU
821	5.220	Master	LE LL	0	22261µs	0	False	232	Empty PDU
822	5.220	Slave	LE LL	0	150µs	0	False	232	Empty PDU
823	5.242	Master	LE LL	0	22263µs	1	False	233	Empty PDU
824	5.242	Slave	LE LL	0	150µs	1	False	233	Empty PDU
825	5.265	Master	LE LL	0	22262µs	0	False	234	Empty PDU
826	5.265	Slave	LE LL	0	150µs	0	False	234	Empty PDU
827	5.287	Master	LE LL	0	22262µs	1	False	235	Empty PDU
828	5.287	Slave	LE LL	0	150µs	1	False	235	Empty PDU
829	5.310	Master	LE LL	0	22264µs	0	False	236	Empty PDU
830	5.310	Slave	LE LL	0	150µs	0	False	236	Empty PDU
831	5.332	Master	LE LL	0	22262µs	1	False	237	Empty PDU
832	5.332	Slave	LE LL	0	151µs	1	False	237	Empty PDU
833	5.355	Master	LE LL	0	22262µs	0	False	238	Empty PDU
834	5.355	Slave	LE LL	0	150µs	0	False	238	Empty PDU
835	5.377	Master	LE LL	0	22262µs	1	False	239	Empty PDU
836	5.377	Slave	LE LL	0	150µs	1	False	239	Empty PDU
837	5.400	Master	LE LL	0	22263µs	0	False	240	Empty PDU
838	5.400	Slave	LE LL	0	150µs	0	False	240	Empty PDU
839	5.422	Master	LE LL	0	22262µs	1	False	241	Empty PDU
840	5.422	Slave	LE LL	0	150µs	1	False	241	Empty PDU
841	5.445	Master	LE LL	0	22262µs	0	False	242	Empty PDU
842	5.445	Slave	LE LL	0	150µs	0	False	242	Empty PDU
843	5.467	Master	LE LL	0	22262µs	1	False	243	Empty PDU

844	5.467	Slave	LE LL	0	150µs	1	False	243	Empty PDU
845	5.490	Master	LE LL	0	22263µs	0	False	244	Empty PDU
846	5.490	Slave	LE LL	0	150µs	0	False	244	Empty PDU
847	5.512	Master	LE LL	0	22262µs	1	False	245	Empty PDU
848	5.512	Slave	LE LL	0	150µs	1	False	245	Empty PDU
849	5.535	Master	LE LL	0	22262µs	0	False	246	Empty PDU
850	5.535	Slave	LE LL	0	150µs	0	False	246	Empty PDU
851	5.557	Master	LE LL	0	22263µs	1	False	247	Empty PDU
852	5.557	Slave	LE LL	0	151µs	1	False	247	Empty PDU
853	5.580	Master	LE LL	0	22262µs	0	False	248	Empty PDU
854	5.580	Slave	LE LL	0	150µs	0	False	248	Empty PDU
855	5.602	Master	LE LL	0	22261µs	1	False	249	Empty PDU
856	5.602	Slave	LE LL	0	150µs	1	False	249	Empty PDU
857	5.625	Master	LE LL	0	22263µs	0	False	250	Empty PDU
858	5.625	Slave	LE LL	0	149µs	0	False	250	Empty PDU
859	5.647	Master	LE LL	0	22262µs	1	False	251	Empty PDU
860	5.647	Slave	LE LL	0	150µs	1	False	251	Empty PDU
861	5.670	Master	LE LL	0	22262µs	0	False	252	Empty PDU
862	5.670	Slave	LE LL	0	150µs	0	False	252	Empty PDU
863	5.692	Master	LE LL	0	22263µs	1	False	253	Empty PDU
864	5.692	Slave	LE LL	0	150µs	1	False	253	Empty PDU
865	5.715	Master	LE LL	0	22262µs	0	False	254	Empty PDU
866	5.715	Slave	LE LL	0	150µs	0	False	254	Empty PDU
867	5.737	Master	LE LL	0	22263µs	1	False	255	Empty PDU
868	5.737	Slave	LE LL	0	150µs	1	False	255	Empty PDU
869	5.760	Master	LE LL	0	22263µs	0	False	256	Empty PDU
870	5.760	Slave	LE LL	0	150µs	0	False	256	Empty PDU
871	5.782	Master	LE LL	0	22262µs	1	False	257	Empty PDU
872	5.782	Slave	LE LL	0	150µs	1	False	257	Empty PDU
873	5.805	Master	LE LL	0	22262µs	0	False	258	Empty PDU
874	5.805	Slave	LE LL	0	150µs	0	False	258	Empty PDU
875	5.827	Master	LE LL	0	22261µs	1	False	259	Empty PDU
876	5.827	Slave	LE LL	0	150µs	1	False	259	Empty PDU
877	5.850	Master	LE LL	0	22263µs	0	False	260	Empty PDU
878	5.850	Slave	LE LL	0	150µs	0	False	260	Empty PDU
879	5.872	Master	LE LL	0	22263µs	1	False	261	Empty PDU
880	5.872	Slave	LE LL	0	149µs	1	False	261	Empty PDU
881	5.895	Master	LE LL	0	22262µs	0	False	262	Empty PDU
882	5.895	Slave	LE LL	0	150µs	0	False	262	Empty PDU
883	5.917	Master	LE LL	0	22262µs	1	False	263	Empty PDU
884	5.917	Slave	LE LL	0	149µs	1	False	263	Empty PDU
885	5.940	Master	LE LL	0	22264µs	0	False	264	Empty PDU
886	5.940	Slave	LE LL	0	150µs	0	False	264	Empty PDU
887	5.962	Master	LE LL	0	22262µs	1	False	265	Empty PDU
888	5.962	Slave	LE LL	0	150µs	1	False	265	Empty PDU

889	5.985	Master	LE LL	0	22262µs	0	False	266	Empty PDU
890	5.985	Slave	LE LL	0	150µs	0	False	266	Empty PDU
891	6.007	Master	LE LL	0	22263µs	1	False	267	Empty PDU
892	6.007	Slave	LE LL	0	149µs	1	False	267	Empty PDU
893	6.030	Master	LE LL	0	22263µs	0	False	268	Empty PDU
894	6.030	Slave	LE LL	0	150µs	0	False	268	Empty PDU
895	6.052	Master	LE LL	0	22262µs	1	False	269	Empty PDU
896	6.052	Slave	LE LL	0	150µs	1	False	269	Empty PDU
897	6.075	Master	LE LL	0	22262µs	0	False	270	Empty PDU
898	6.075	Slave	LE LL	0	150µs	0	False	270	Empty PDU
899	6.097	Master	LE LL	0	22262µs	1	False	271	Empty PDU
900	6.097	Slave	LE LL	0	149µs	1	False	271	Empty PDU
901	6.120	Master	LE LL	0	22264µs	0	False	272	Empty PDU
902	6.120	Slave	LE LL	0	150µs	0	False	272	Empty PDU
903	6.142	Master	LE LL	0	22262µs	1	False	273	Empty PDU
904	6.142	Slave	LE LL	0	150µs	1	False	273	Empty PDU
905	6.165	Master	LE LL	0	22262µs	0	False	274	Empty PDU
906	6.165	Slave	LE LL	0	150µs	0	False	274	Empty PDU
907	6.187	Master	LE LL	0	22262µs	1	False	275	Empty PDU
908	6.187	Slave	LE LL	0	150µs	1	False	275	Empty PDU
909	6.210	Master	LE LL	0	22263µs	0	False	276	Empty PDU
910	6.210	Slave	LE LL	0	150µs	0	False	276	Empty PDU
911	6.232	Master	LE LL	0	22262µs	1	False	277	Empty PDU
912	6.232	Slave	LE LL	0	150µs	1	False	277	Empty PDU
913	6.255	Master	LE LL	0	22262µs	0	False	278	Empty PDU
914	6.255	Slave	LE LL	0	150µs	0	False	278	Empty PDU
915	6.277	Master	LE LL	0	22262µs	1	False	279	Empty PDU
916	6.277	Slave	LE LL	0	149µs	1	False	279	Empty PDU
917	6.300	Master	LE LL	0	22264µs	0	False	280	Empty PDU
918	6.300	Slave	LE LL	0	150µs	0	False	280	Empty PDU
919	6.322	Master	LE LL	0	22262µs	1	False	281	Empty PDU
920	6.322	Slave	LE LL	0	150µs	1	False	281	Empty PDU
921	6.345	Master	LE LL	0	22261µs	0	False	282	Empty PDU
922	6.345	Slave	LE LL	81	151µs	1	True	282	L2CAP Fragment[BoundErrorUnreassembled Packet]
923	6.367	Master	LE LL	0	21938µs	1	False	283	Empty PDU
924	6.367	Slave	LE LL	0	150µs	1	False	283	Empty PDU
925	6.390	Master	LE LL	0	22262µs	0	False	284	Empty PDU
926	6.390	Slave	LE LL	0	150µs	0	False	284	Empty PDU
927	6.412	Master	LE LL	0	22263µs	1	False	285	Empty PDU
928	6.412	Slave	LE LL	0	149µs	1	False	285	Empty PDU
929	6.457	Master	LE LL	0	44763µs	0	False	287	Empty PDU
930	6.457	Slave	LE LL	0	150µs	0	False	287	Empty PDU
931	6.480	Master	LE LL	0	22261µs	1	False	288	Empty PDU
932	6.480	Slave	LE LL	0	150µs	1	False	288	Empty PDU
933	6.502	Master	LE LL	0	22262µs	0	False	289	Empty PDU

934	6.502	Slave	LE LL	0	150µs	0	False	289	Empty PDU
935	6.525	Master	LE LL	0	22262µs	1	False	290	Empty PDU
936	6.525	Slave	LE LL	0	151µs	1	False	290	Empty PDU
937	6.547	Master	LE LL	0	22262µs	0	False	291	Empty PDU
938	6.547	Slave	LE LL	0	150µs	0	False	291	Empty PDU
939	6.570	Master	LE LL	0	22263µs	1	False	292	Empty PDU
940	6.570	Slave	LE LL	0	150µs	1	False	292	Empty PDU
941	6.592	Master	ATT	106	22262µs	0	False	293	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
942	6.593	Slave	LE LL	0	150µs	0	False	293	Empty PDU
943	6.615	Master	LE LL	0	21839µs	1	False	294	Empty PDU
944	6.615	Slave	ATT	5	150µs	1	True	294	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
945	6.615	Master	LE LL	0	150µs	0	False	294	Empty PDU
946	6.615	Slave	LE LL	0	150µs	0	False	294	Empty PDU
947	6.637	Master	LE LL	0	21854µs	1	False	295	Empty PDU
948	6.637	Slave	LE LL	0	150µs	1	False	295	Empty PDU
949	6.660	Master	LE LL	0	22262µs	0	False	296	Empty PDU
950	6.660	Slave	LE LL	0	149µs	0	False	296	Empty PDU
951	6.682	Master	LE LL	0	22264µs	1	False	297	Empty PDU
952	6.682	Slave	LE LL	0	150µs	1	False	297	Empty PDU
953	6.705	Master	LE LL	0	22262µs	0	False	298	Empty PDU
954	6.705	Slave	LE LL	0	150µs	0	False	298	Empty PDU
955	6.727	Master	LE LL	0	22263µs	1	False	299	Empty PDU
956	6.727	Slave	LE LL	0	150µs	1	False	299	Empty PDU
957	6.750	Master	LE LL	0	22261µs	0	False	300	Empty PDU
958	6.750	Slave	LE LL	0	150µs	0	False	300	Empty PDU
959	6.772	Master	LE LL	0	22263µs	1	False	301	Empty PDU
960	6.772	Slave	LE LL	0	150µs	1	False	301	Empty PDU
961	6.795	Master	LE LL	0	22261µs	0	False	302	Empty PDU
962	6.795	Slave	LE LL	0	150µs	0	False	302	Empty PDU
963	6.817	Master	LE LL	0	22262µs	1	False	303	Empty PDU
964	6.817	Slave	LE LL	0	150µs	1	False	303	Empty PDU
965	6.840	Master	LE LL	0	22263µs	0	False	304	Empty PDU
966	6.840	Slave	LE LL	0	150µs	0	False	304	Empty PDU
967	6.862	Master	LE LL	0	22261µs	1	False	305	Empty PDU
968	6.862	Slave	LE LL	0	150µs	1	False	305	Empty PDU
969	6.885	Master	LE LL	0	22263µs	0	False	306	Empty PDU
970	6.885	Slave	LE LL	0	150µs	0	False	306	Empty PDU
971	6.907	Master	LE LL	0	22262µs	1	False	307	Empty PDU
972	6.907	Slave	LE LL	0	150µs	1	False	307	Empty PDU
973	6.930	Master	LE LL	0	22263µs	0	False	308	Empty PDU
974	6.930	Slave	LE LL	0	149µs	0	False	308	Empty PDU
975	6.952	Master	LE LL	0	22263µs	1	False	309	Empty PDU
976	6.952	Slave	LE LL	0	150µs	1	False	309	Empty PDU
977	6.975	Master	LE LL	0	22262µs	0	False	310	Empty PDU
978	6.975	Slave	LE LL	0	150µs	0	False	310	Empty PDU

979	6.997	Master	LE LL	0	22262µs	1	False	311	Empty PDU
980	6.997	Slave	LE LL	0	150µs	1	False	311	Empty PDU
981	7.020	Master	LE LL	0	22263µs	0	False	312	Empty PDU
982	7.020	Slave	LE LL	0	150µs	0	False	312	Empty PDU
983	7.042	Master	LE LL	0	22262µs	1	False	313	Empty PDU
984	7.042	Slave	LE LL	0	150µs	1	False	313	Empty PDU
985	7.065	Master	LE LL	0	22263µs	0	False	314	Empty PDU
986	7.065	Slave	LE LL	0	150µs	0	False	314	Empty PDU
987	7.087	Master	LE LL	0	22262µs	1	False	315	Empty PDU
988	7.087	Slave	LE LL	0	150µs	1	False	315	Empty PDU
989	7.110	Master	LE LL	0	22261µs	0	False	316	Empty PDU
990	7.110	Slave	LE LL	0	150µs	0	False	316	Empty PDU
991	7.132	Master	LE LL	0	22263µs	1	False	317	Empty PDU
992	7.132	Slave	LE LL	0	150µs	1	False	317	Empty PDU
993	7.155	Master	LE LL	0	22261µs	0	False	318	Empty PDU
994	7.155	Slave	LE LL	0	150µs	0	False	318	Empty PDU
995	7.177	Master	LE LL	0	22264µs	1	False	319	Empty PDU
996	7.177	Slave	LE LL	0	150µs	1	False	319	Empty PDU
997	7.200	Master	LE LL	0	22261µs	0	False	320	Empty PDU
998	7.200	Slave	LE LL	0	150µs	0	False	320	Empty PDU
999	7.222	Master	LE LL	0	22263µs	1	False	321	Empty PDU
1000	7.222	Slave	LE LL	0	151µs	1	False	321	Empty PDU
1001	7.245	Master	LE LL	0	22262µs	0	False	322	Empty PDU
1002	7.245	Slave	LE LL	0	150µs	0	False	322	Empty PDU
1003	7.267	Master	LE LL	0	22261µs	1	False	323	Empty PDU
1004	7.267	Slave	LE LL	0	150µs	1	False	323	Empty PDU
1005	7.290	Master	LE LL	0	22262µs	0	False	324	Empty PDU
1006	7.290	Slave	LE LL	27	150µs	0	True	324	L2CAP Fragment Start
1007	7.290	Master	LE LL	0	150µs	1	False	324	Empty PDU
1008	7.290	Slave	LE LL	27	150µs	1	True	324	L2CAP Fragment
1009	7.291	Master	LE LL	0	150µs	0	False	324	Empty PDU
1010	7.291	Slave	LE LL	27	150µs	0	True	324	L2CAP Fragment
1011	7.291	Master	LE LL	0	150µs	1	False	324	Empty PDU
1012	7.291	Slave	LE LL	27	150µs	1	True	324	L2CAP Fragment
1013	7.292	Master	LE LL	0	150µs	0	False	324	Empty PDU
1014	7.292	Slave	LE LL	27	150µs	0	True	324	L2CAP Fragment
1015	7.292	Master	LE LL	0	150µs	1	False	324	Empty PDU
1016	7.292	Slave	LE LL	27	150µs	1	True	324	L2CAP Fragment
1017	7.293	Master	LE LL	0	150µs	0	False	324	Empty PDU
1018	7.293	Slave	LE LL	27	150µs	0	True	324	L2CAP Fragment
1019	7.293	Master	LE LL	0	150µs	1	False	324	Empty PDU
1020	7.293	Slave	LE LL	27	150µs	1	True	324	L2CAP Fragment
1021	7.294	Master	LE LL	0	150µs	0	False	324	Empty PDU
1022	7.294	Slave	LE LL	27	150µs	0	True	324	L2CAP Fragment
1023	7.294	Master	LE LL	0	150µs	1	False	324	Empty PDU

1024	7.294	Slave	LE LL	8	150µs	1	True	324	L2CAP Fragment
1025	7.295	Master	LE LL	0	150µs	0	False	324	Empty PDU
1026	7.295	Slave	LE LL	0	150µs	0	False	324	Empty PDU
1027	7.312	Master	ATT	5	17378µs	1	False	325	Sent Handle Value Confirmation
1028	7.312	Slave	LE LL	0	151µs	1	False	325	Empty PDU
1029	7.335	Master	LE LL	0	22243µs	0	False	326	Empty PDU
1030	7.335	Slave	LE LL	27	150µs	0	True	326	L2CAP Fragment Start
1031	7.335	Master	LE LL	0	150µs	1	False	326	Empty PDU
1032	7.335	Slave	LE LL	27	150µs	1	True	326	L2CAP Fragment
1033	7.336	Master	LE LL	0	150µs	0	False	326	Empty PDU
1034	7.336	Slave	LE LL	27	150µs	0	True	326	L2CAP Fragment
1035	7.336	Master	LE LL	0	150µs	1	False	326	Empty PDU
1036	7.336	Slave	LE LL	27	150µs	1	True	326	L2CAP Fragment
1037	7.337	Master	LE LL	0	150µs	0	False	326	Empty PDU
1038	7.337	Slave	LE LL	27	150µs	0	True	326	L2CAP Fragment
1039	7.337	Master	LE LL	0	150µs	1	False	326	Empty PDU
1040	7.337	Slave	LE LL	10	150µs	1	True	326	L2CAP Fragment
1041	7.338	Master	LE LL	0	150µs	0	False	326	Empty PDU
1042	7.338	Slave	LE LL	0	150µs	0	False	326	Empty PDU
1043	7.357	Master	ATT	5	19354µs	1	False	327	Sent Handle Value Confirmation
1044	7.357	Slave	LE LL	0	150µs	1	False	327	Empty PDU
1045	7.380	Master	LE LL	0	22242µs	0	False	328	Empty PDU
1046	7.380	Slave	LE LL	0	150µs	0	False	328	Empty PDU
1047	7.402	Master	ATT	251	22262µs	1	False	329	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1048	7.403	Slave	LE LL	0	150µs	1	False	329	Empty PDU
1049	7.425	Master	LE LL	0	21258µs	0	False	330	Empty PDU
1050	7.425	Slave	ATT	5	150µs	0	True	330	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1051	7.425	Master	LE LL	0	150µs	1	False	330	Empty PDU
1052	7.425	Slave	LE LL	0	150µs	1	False	330	Empty PDU
1053	7.447	Master	ATT	81	21854µs	0	False	331	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1054	7.448	Slave	LE LL	0	150µs	0	False	331	Empty PDU
1055	7.470	Master	LE LL	0	21939µs	1	False	332	Empty PDU
1056	7.470	Slave	ATT	5	150µs	1	True	332	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1057	7.470	Master	LE LL	0	150µs	0	False	332	Empty PDU
1058	7.470	Slave	LE LL	0	150µs	0	False	332	Empty PDU
1059	7.492	Master	LE LL	0	21855µs	1	False	333	Empty PDU
1060	7.492	Slave	LE LL	0	150µs	1	False	333	Empty PDU
1061	7.515	Master	LE LL	0	22262µs	0	False	334	Empty PDU
1062	7.515	Slave	LE LL	0	150µs	0	False	334	Empty PDU
1063	7.537	Master	LE LL	0	22261µs	1	False	335	Empty PDU
1064	7.537	Slave	LE LL	0	150µs	1	False	335	Empty PDU
1065	7.560	Master	LE LL	0	22262µs	0	False	336	Empty PDU
1066	7.560	Slave	LE LL	0	150µs	0	False	336	Empty PDU
1067	7.582	Master	LE LL	0	22264µs	1	False	337	Empty PDU
1068	7.582	Slave	LE LL	0	150µs	1	False	337	Empty PDU

1069	7.605	Master	LE LL	0	22262µs	0	False	338	Empty PDU
1070	7.605	Slave	LE LL	0	150µs	0	False	338	Empty PDU
1071	7.627	Master	LE LL	0	22261µs	1	False	339	Empty PDU
1072	7.627	Slave	LE LL	0	150µs	1	False	339	Empty PDU
1073	7.650	Master	LE LL	0	22263µs	0	False	340	Empty PDU
1074	7.650	Slave	LE LL	0	150µs	0	False	340	Empty PDU
1075	7.672	Master	LE LL	0	22262µs	1	False	341	Empty PDU
1076	7.672	Slave	LE LL	0	150µs	1	False	341	Empty PDU
1077	7.695	Master	LE LL	0	22263µs	0	False	342	Empty PDU
1078	7.695	Slave	LE LL	0	150µs	0	False	342	Empty PDU
1079	7.717	Master	LE LL	0	22261µs	1	False	343	Empty PDU
1080	7.717	Slave	LE LL	0	150µs	1	False	343	Empty PDU
1081	7.740	Master	LE LL	0	22262µs	0	False	344	Empty PDU
1082	7.740	Slave	LE LL	0	150µs	0	False	344	Empty PDU
1083	7.762	Master	LE LL	0	22264µs	1	False	345	Empty PDU
1084	7.762	Slave	LE LL	0	149µs	1	False	345	Empty PDU
1085	7.785	Master	LE LL	0	22262µs	0	False	346	Empty PDU
1086	7.785	Slave	LE LL	0	150µs	0	False	346	Empty PDU
1087	7.807	Master	LE LL	0	22262µs	1	False	347	Empty PDU
1088	7.807	Slave	LE LL	0	150µs	1	False	347	Empty PDU
1089	7.830	Master	LE LL	0	22262µs	0	False	348	Empty PDU
1090	7.830	Slave	LE LL	0	150µs	0	False	348	Empty PDU
1091	7.852	Master	LE LL	0	22263µs	1	False	349	Empty PDU
1092	7.852	Slave	LE LL	0	149µs	1	False	349	Empty PDU
1093	7.875	Master	LE LL	0	22264µs	0	False	350	Empty PDU
1094	7.875	Slave	LE LL	0	150µs	0	False	350	Empty PDU
1095	7.897	Master	LE LL	0	22262µs	1	False	351	Empty PDU
1096	7.897	Slave	LE LL	0	150µs	1	False	351	Empty PDU
1097	7.920	Master	LE LL	0	22262µs	0	False	352	Empty PDU
1098	7.920	Slave	LE LL	0	150µs	0	False	352	Empty PDU
1099	7.942	Master	LE LL	0	22263µs	1	False	353	Empty PDU
1100	7.942	Slave	LE LL	27	149µs	1	True	353	L2CAP Fragment Start
1101	7.943	Master	LE LL	0	151µs	0	False	353	Empty PDU
1102	7.943	Slave	LE LL	27	149µs	0	True	353	L2CAP Fragment
1103	7.943	Master	LE LL	0	151µs	1	False	353	Empty PDU
1104	7.943	Slave	LE LL	21	149µs	1	True	353	L2CAP Fragment
1105	7.944	Master	LE LL	0	151µs	0	False	353	Empty PDU
1106	7.944	Slave	LE LL	0	149µs	0	False	353	Empty PDU
1107	7.965	Master	ATT	5	20798µs	1	True	354	Sent Handle Value Confirmation
1108	7.965	Slave	LE LL	0	150µs	1	False	354	Empty PDU
1109	7.965	Master	ATT	251	150µs	0	False	354	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1110	7.966	Slave	LE LL	0	150µs	0	False	354	Empty PDU
1111	7.987	Master	LE LL	0	20850µs	1	False	355	Empty PDU
1112	7.987	Slave	ATT	5	150µs	1	True	355	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1113	7.988	Master	LE LL	0	150µs	0	False	355	Empty PDU

1114	7.988	Slave	LE LL	0	150µs	0	False	355	Empty PDU
1115	8.010	Master	ATT	121	21854µs	1	False	356	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1116	8.010	Slave	LE LL	0	150µs	1	False	356	Empty PDU
1117	8.032	Master	LE LL	0	21780µs	0	False	357	Empty PDU
1118	8.032	Slave	ATT	5	150µs	0	True	357	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1119	8.033	Master	LE LL	0	150µs	1	False	357	Empty PDU
1120	8.033	Slave	LE LL	0	149µs	1	False	357	Empty PDU
1121	8.055	Master	LE LL	0	21854µs	0	False	358	Empty PDU
1122	8.055	Slave	LE LL	0	150µs	0	False	358	Empty PDU
1123	8.077	Master	LE LL	0	22262µs	1	False	359	Empty PDU
1124	8.077	Slave	LE LL	0	150µs	1	False	359	Empty PDU
1125	8.100	Master	LE LL	0	22263µs	0	False	360	Empty PDU
1126	8.100	Slave	LE LL	0	150µs	0	False	360	Empty PDU
1127	8.122	Master	LE LL	0	22262µs	1	False	361	Empty PDU
1128	8.122	Slave	LE LL	0	150µs	1	False	361	Empty PDU
1129	8.145	Master	LE LL	0	22263µs	0	False	362	Empty PDU
1130	8.145	Slave	LE LL	0	150µs	0	False	362	Empty PDU
1131	8.167	Master	LE LL	0	22262µs	1	False	363	Empty PDU
1132	8.167	Slave	LE LL	0	150µs	1	False	363	Empty PDU
1133	8.190	Master	LE LL	0	22263µs	0	False	364	Empty PDU
1134	8.190	Slave	LE LL	0	150µs	0	False	364	Empty PDU
1135	8.212	Master	LE LL	0	22260µs	1	False	365	Empty PDU
1136	8.212	Slave	LE LL	0	150µs	1	False	365	Empty PDU
1137	8.235	Master	LE LL	0	22263µs	0	False	366	Empty PDU
1138	8.235	Slave	LE LL	0	151µs	0	False	366	Empty PDU
1139	8.257	Master	LE LL	0	22261µs	1	False	367	Empty PDU
1140	8.257	Slave	LE LL	0	149µs	1	False	367	Empty PDU
1141	8.280	Master	LE LL	0	22263µs	0	False	368	Empty PDU
1142	8.280	Slave	LE LL	0	150µs	0	False	368	Empty PDU
1143	8.302	Master	LE LL	0	22262µs	1	False	369	Empty PDU
1144	8.302	Slave	LE LL	0	149µs	1	False	369	Empty PDU
1145	8.325	Master	LE LL	0	22263µs	0	False	370	Empty PDU
1146	8.325	Slave	LE LL	0	150µs	0	False	370	Empty PDU
1147	8.347	Master	LE LL	0	22263µs	1	False	371	Empty PDU
1148	8.347	Slave	LE LL	0	150µs	1	False	371	Empty PDU
1149	8.370	Master	LE LL	0	22261µs	0	False	372	Empty PDU
1150	8.370	Slave	LE LL	0	150µs	0	False	372	Empty PDU
1151	8.392	Master	LE LL	0	22263µs	1	False	373	Empty PDU
1152	8.392	Slave	LE LL	0	150µs	1	False	373	Empty PDU
1153	8.415	Master	LE LL	0	22263µs	0	False	374	Empty PDU
1154	8.415	Slave	LE LL	0	150µs	0	False	374	Empty PDU
1155	8.437	Master	LE LL	0	22261µs	1	False	375	Empty PDU
1156	8.437	Slave	LE LL	0	150µs	1	False	375	Empty PDU
1157	8.460	Master	LE LL	0	22263µs	0	False	376	Empty PDU
1158	8.460	Slave	LE LL	0	150µs	0	False	376	Empty PDU

1159	8.482	Master	LE LL	0	22263µs	1	False	377	Empty PDU
1160	8.482	Slave	LE LL	0	150µs	1	False	377	Empty PDU
1161	8.505	Master	LE LL	0	22261µs	0	False	378	Empty PDU
1162	8.505	Slave	LE LL	0	150µs	0	False	378	Empty PDU
1163	8.527	Master	LE LL	0	22263µs	1	False	379	Empty PDU
1164	8.527	Slave	LE LL	0	150µs	1	False	379	Empty PDU
1165	8.550	Master	LE LL	0	22263µs	0	False	380	Empty PDU
1166	8.550	Slave	LE LL	0	150µs	0	False	380	Empty PDU
1167	8.572	Master	LE LL	0	22262µs	1	False	381	Empty PDU
1168	8.572	Slave	LE LL	0	150µs	1	False	381	Empty PDU
1169	8.595	Master	LE LL	0	22261µs	0	False	382	Empty PDU
1170	8.595	Slave	LE LL	27	150µs	0	True	382	L2CAP Fragment Start
1171	8.595	Master	LE LL	0	150µs	1	False	382	Empty PDU
1172	8.595	Slave	LE LL	27	150µs	1	True	382	L2CAP Fragment
1173	8.596	Master	LE LL	0	150µs	0	False	382	Empty PDU
1174	8.596	Slave	LE LL	24	150µs	0	True	382	L2CAP Fragment
1175	8.596	Master	LE LL	0	150µs	1	False	382	Empty PDU
1176	8.596	Slave	LE LL	0	150µs	1	False	382	Empty PDU
1177	8.617	Master	ATT	5	20786µs	0	True	383	Sent Handle Value Confirmation
1178	8.617	Slave	LE LL	0	150µs	0	False	383	Empty PDU
1179	8.618	Master	ATT	109	150µs	1	False	383	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1180	8.618	Slave	LE LL	0	150µs	1	False	383	Empty PDU
1181	8.640	Master	LE LL	0	21419µs	0	False	384	Empty PDU
1182	8.640	Slave	ATT	5	150µs	0	True	384	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1183	8.640	Master	LE LL	0	150µs	1	False	384	Empty PDU
1184	8.640	Slave	LE LL	0	150µs	1	False	384	Empty PDU
1185	8.662	Master	LE LL	0	21855µs	0	False	385	Empty PDU
1186	8.662	Slave	LE LL	0	150µs	0	False	385	Empty PDU
1187	8.685	Master	LE LL	0	22261µs	1	False	386	Empty PDU
1188	8.685	Slave	LE LL	0	150µs	1	False	386	Empty PDU
1189	8.707	Master	LE LL	0	22263µs	0	False	387	Empty PDU
1190	8.707	Slave	LE LL	27	150µs	0	True	387	L2CAP Fragment Start
1191	8.708	Master	LE LL	0	150µs	1	False	387	Empty PDU
1192	8.708	Slave	LE LL	27	149µs	1	True	387	L2CAP Fragment
1193	8.708	Master	LE LL	0	151µs	0	False	387	Empty PDU
1194	8.708	Slave	LE LL	24	149µs	0	True	387	L2CAP Fragment
1195	8.730	Master	LE LL	0	21176µs	1	True	388	Empty PDU
1196	8.730	Slave	LE LL	0	149µs	1	False	388	Empty PDU
1197	8.730	Master	ATT	5	151µs	0	True	388	Sent Handle Value Confirmation
1198	8.730	Slave	LE LL	0	149µs	0	False	388	Empty PDU
1199	8.730	Master	ATT	77	151µs	1	False	388	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1200	8.731	Slave	LE LL	0	149µs	1	False	388	Empty PDU
1201	8.752	Master	LE LL	0	21158µs	0	False	389	Empty PDU
1202	8.752	Slave	ATT	5	150µs	0	True	389	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1203	8.753	Master	LE LL	0	150µs	1	False	389	Empty PDU

1204	8.753	Slave	LE LL	0	150µs	1	False	389	Empty PDU
1205	8.775	Master	LE LL	0	21854µs	0	False	390	Empty PDU
1206	8.775	Slave	LE LL	0	150µs	0	False	390	Empty PDU
1207	8.797	Master	LE LL	0	22264µs	1	False	391	Empty PDU
1208	8.797	Slave	LE LL	0	150µs	1	False	391	Empty PDU
1209	8.820	Master	LE LL	0	22261µs	0	False	392	Empty PDU
1210	8.820	Slave	LE LL	27	149µs	0	True	392	L2CAP Fragment Start
1211	8.820	Master	LE LL	0	151µs	1	False	392	Empty PDU
1212	8.820	Slave	LE LL	27	149µs	1	True	392	L2CAP Fragment
1213	8.821	Master	LE LL	0	151µs	0	False	392	Empty PDU
1214	8.821	Slave	LE LL	24	149µs	0	True	392	L2CAP Fragment
1215	8.821	Master	LE LL	0	151µs	1	False	392	Empty PDU
1216	8.821	Slave	LE LL	0	149µs	1	False	392	Empty PDU
1217	8.842	Master	ATT	5	20788µs	0	True	393	Sent Handle Value Confirmation
1218	8.842	Slave	LE LL	0	150µs	0	False	393	Empty PDU
1219	8.843	Master	ATT	90	150µs	1	False	393	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1220	8.843	Slave	LE LL	0	150µs	1	False	393	Empty PDU
1221	8.865	Master	LE LL	0	21493µs	0	False	394	Empty PDU
1222	8.865	Slave	ATT	5	150µs	0	True	394	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1223	8.865	Master	LE LL	0	150µs	1	False	394	Empty PDU
1224	8.865	Slave	LE LL	0	150µs	1	False	394	Empty PDU
1225	8.887	Master	LE LL	0	21854µs	0	False	395	Empty PDU
1226	8.887	Slave	LE LL	0	150µs	0	False	395	Empty PDU
1227	8.910	Master	LE LL	0	22264µs	1	False	396	Empty PDU
1228	8.910	Slave	LE LL	0	150µs	1	False	396	Empty PDU
1229	8.932	Master	LE LL	0	22262µs	0	False	397	Empty PDU
1230	8.955	Master	LE LL	0	22455µs	0	False	398	Empty PDU
1231	8.977	Master	LE LL	0	22458µs	0	False	399	Empty PDU
1232	8.977	Slave	LE LL	0	150µs	0	False	399	Empty PDU
1233	9.000	Master	LE LL	0	22261µs	1	False	400	Empty PDU
1234	9.022	Master	LE LL	0	22456µs	1	False	401	Empty PDU
1235	9.045	Master	LE LL	0	22457µs	1	False	402	Empty PDU
1236	9.045	Slave	LE LL	0	149µs	1	False	402	Empty PDU
1237	9.067	Master	LE LL	0	22264µs	0	False	403	Empty PDU
1238	9.067	Slave	LE LL	0	150µs	0	False	403	Empty PDU
1239	9.090	Master	LE LL	0	22261µs	1	False	404	Empty PDU
1240	9.090	Slave	LE LL	0	150µs	1	False	404	Empty PDU
1241	9.112	Master	LE LL	0	22262µs	0	False	405	Empty PDU
1242	9.112	Slave	LE LL	0	150µs	0	False	405	Empty PDU
1243	9.135	Master	LE LL	0	22263µs	1	False	406	Empty PDU
1244	9.135	Slave	LE LL	0	149µs	1	False	406	Empty PDU
1245	9.157	Master	LE LL	0	22263µs	0	False	407	Empty PDU
1246	9.157	Slave	LE LL	0	150µs	0	False	407	Empty PDU
1247	9.180	Master	LE LL	0	22263µs	1	False	408	Empty PDU
1248	9.202	Master	LE LL	0	22455µs	1	False	409	Empty PDU

1249	9.225	Master	LE LL	0	22457µs	1	False	410	Empty PDU
1250	9.225	Slave	LE LL	0	150µs	1	False	410	Empty PDU
1251	9.247	Master	LE LL	0	22263µs	0	False	411	Empty PDU
1252	9.270	Master	LE LL	0	22456µs	0	False	412	Empty PDU
1253	9.292	Master	LE LL	0	22455µs	0	False	413	Empty PDU
1254	9.292	Slave	LE LL	0	150µs	0	False	413	Empty PDU
1255	9.315	Master	LE LL	0	22263µs	1	False	414	Empty PDU
1256	9.315	Slave	LE LL	0	150µs	1	False	414	Empty PDU
1257	9.337	Master	LE LL	0	22261µs	0	False	415	Empty PDU
1258	9.337	Slave	LE LL	0	150µs	0	False	415	Empty PDU
1259	9.360	Master	LE LL	0	22262µs	1	False	416	Empty PDU
1260	9.360	Slave	LE LL	0	150µs	1	False	416	Empty PDU
1261	9.382	Master	LE LL	0	22264µs	0	False	417	Empty PDU
1262	9.382	Slave	LE LL	0	150µs	0	False	417	Empty PDU
1263	9.405	Master	LE LL	0	22262µs	1	False	418	Empty PDU
1264	9.427	Master	LE LL	0	22456µs	1	False	419	Empty PDU
1265	9.450	Master	LE LL	0	22457µs	1	False	420	Empty PDU
1266	9.450	Slave	LE LL	0	150µs	1	False	420	Empty PDU
1267	9.472	Master	LE LL	0	22261µs	0	False	421	Empty PDU
1268	9.495	Master	LE LL	0	22455µs	0	False	422	Empty PDU
1269	9.517	Master	LE LL	0	22457µs	0	False	423	Empty PDU
1270	9.517	Slave	LE LL	0	150µs	0	False	423	Empty PDU
1271	9.540	Master	LE LL	0	22262µs	1	False	424	Empty PDU
1272	9.540	Slave	LE LL	0	150µs	1	False	424	Empty PDU
1273	9.562	Master	LE LL	0	22261µs	0	False	425	Empty PDU
1274	9.562	Slave	LE LL	0	151µs	0	False	425	Empty PDU
1275	9.585	Master	LE LL	0	22263µs	1	False	426	Empty PDU
1276	9.585	Slave	LE LL	0	150µs	1	False	426	Empty PDU
1277	9.607	Master	LE LL	0	22262µs	0	False	427	Empty PDU
1278	9.607	Slave	LE LL	0	150µs	0	False	427	Empty PDU
1279	9.630	Master	LE LL	0	22262µs	1	False	428	Empty PDU
1280	9.630	Slave	LE LL	0	150µs	1	False	428	Empty PDU
1281	9.652	Master	LE LL	0	22263µs	0	False	429	Empty PDU
1282	9.675	Master	LE LL	0	22456µs	0	False	430	Empty PDU
1283	9.697	Master	LE LL	0	22456µs	0	False	431	Empty PDU
1284	9.697	Slave	LE LL	0	151µs	0	False	431	Empty PDU
1285	9.720	Master	LE LL	0	22260µs	1	False	432	Empty PDU
1286	9.742	Master	LE LL	0	22457µs	1	False	433	Empty PDU
1287	9.765	Master	LE LL	0	22456µs	1	False	434	Empty PDU
1288	9.765	Slave	LE LL	0	150µs	1	False	434	Empty PDU
1289	9.787	Master	LE LL	0	22262µs	0	False	435	Empty PDU
1290	9.787	Slave	LE LL	0	150µs	0	False	435	Empty PDU
1291	9.810	Master	LE LL	0	22262µs	1	False	436	Empty PDU
1292	9.810	Slave	LE LL	0	150µs	1	False	436	Empty PDU
1293	9.832	Master	LE LL	0	22262µs	0	False	437	Empty PDU

1294	9.832	Slave	LE LL	0	149µs	0	False	437	Empty PDU
1295	9.855	Master	LE LL	0	22264µs	1	False	438	Empty PDU
1296	9.855	Slave	LE LL	0	150µs	1	False	438	Empty PDU
1297	9.877	Master	LE LL	0	22261µs	0	False	439	Empty PDU
1298	9.877	Slave	LE LL	0	150µs	0	False	439	Empty PDU
1299	9.900	Master	LE LL	0	22263µs	1	False	440	Empty PDU
1300	9.922	Master	LE LL	0	22457µs	1	False	441	Empty PDU
1301	9.945	Master	LE LL	0	22455µs	1	False	442	Empty PDU
1302	9.945	Slave	LE LL	0	150µs	1	False	442	Empty PDU
1303	9.967	Master	LE LL	0	22262µs	0	False	443	Empty PDU
1304	9.990	Master	LE LL	0	22458µs	0	False	444	Empty PDU
1305	10.012	Master	LE LL	0	22455µs	0	False	445	Empty PDU
1306	10.012	Slave	LE LL	0	150µs	0	False	445	Empty PDU
1307	10.035	Master	LE LL	0	22263µs	1	False	446	Empty PDU
1308	10.035	Slave	LE LL	0	150µs	1	False	446	Empty PDU
1309	10.057	Master	LE LL	0	22262µs	0	False	447	Empty PDU
1310	10.057	Slave	LE LL	0	150µs	0	False	447	Empty PDU
1311	10.080	Master	LE LL	0	22262µs	1	False	448	Empty PDU
1312	10.080	Slave	LE LL	0	150µs	1	False	448	Empty PDU
1313	10.102	Master	LE LL	0	22261µs	0	False	449	Empty PDU
1314	10.102	Slave	LE LL	0	150µs	0	False	449	Empty PDU
1315	10.125	Master	LE LL	0	22263µs	1	False	450	Empty PDU
1316	10.147	Master	LE LL	0	22457µs	1	False	451	Empty PDU
1317	10.170	Master	LE LL	0	22456µs	1	False	452	Empty PDU
1318	10.170	Slave	LE LL	0	151µs	1	False	452	Empty PDU
1319	10.192	Master	LE LL	0	22262µs	0	False	453	Empty PDU
1320	10.215	Master	LE LL	0	22456µs	0	False	454	Empty PDU
1321	10.237	Master	LE LL	0	22455µs	0	False	455	Empty PDU
1322	10.237	Slave	LE LL	0	150µs	0	False	455	Empty PDU
1323	10.260	Master	LE LL	0	22262µs	1	False	456	Empty PDU
1324	10.260	Slave	LE LL	0	151µs	1	False	456	Empty PDU
1325	10.282	Master	LE LL	0	22263µs	0	False	457	Empty PDU
1326	10.282	Slave	LE LL	0	149µs	0	False	457	Empty PDU
1327	10.305	Master	LE LL	0	22263µs	1	False	458	Empty PDU
1328	10.305	Slave	LE LL	0	150µs	1	False	458	Empty PDU
1329	10.327	Master	LE LL	0	22261µs	0	False	459	Empty PDU
1330	10.327	Slave	LE LL	0	150µs	0	False	459	Empty PDU
1331	10.350	Master	LE LL	0	22263µs	1	False	460	Empty PDU
1332	10.350	Slave	LE LL	0	151µs	1	False	460	Empty PDU
1333	10.372	Master	LE LL	0	22262µs	0	False	461	Empty PDU
1334	10.395	Master	LE LL	0	22455µs	0	False	462	Empty PDU
1335	10.417	Master	LE LL	0	22456µs	0	False	463	Empty PDU
1336	10.417	Slave	LE LL	0	150µs	0	False	463	Empty PDU
1337	10.440	Master	LE LL	0	22264µs	1	False	464	Empty PDU
1338	10.462	Master	LE LL	0	22455µs	1	False	465	Empty PDU

1339	10.485	Master	LE LL	0	22456µs	1	False	466	Empty PDU
1340	10.485	Slave	LE LL	0	150µs	1	False	466	Empty PDU
1341	10.507	Master	LE LL	0	22263µs	0	False	467	Empty PDU
1342	10.507	Slave	LE LL	0	150µs	0	False	467	Empty PDU
1343	10.530	Master	LE LL	0	22262µs	1	False	468	Empty PDU
1344	10.530	Slave	LE LL	0	151µs	1	False	468	Empty PDU
1345	10.552	Master	LE LL	0	22262µs	0	False	469	Empty PDU
1346	10.552	Slave	LE LL	0	149µs	0	False	469	Empty PDU
1347	10.575	Master	LE LL	0	22263µs	1	False	470	Empty PDU
1348	10.575	Slave	LE LL	0	150µs	1	False	470	Empty PDU
1349	10.597	Master	LE LL	0	22261µs	0	False	471	Empty PDU
1350	10.597	Slave	LE LL	0	150µs	0	False	471	Empty PDU
1351	10.620	Master	LE LL	0	22263µs	1	False	472	Empty PDU
1352	10.642	Master	LE LL	0	22456µs	1	False	473	Empty PDU
1353	10.665	Master	LE LL	0	22457µs	1	False	474	Empty PDU
1354	10.665	Slave	LE LL	0	150µs	1	False	474	Empty PDU
1355	10.687	Master	LE LL	0	22262µs	0	False	475	Empty PDU
1356	10.710	Master	LE LL	0	22455µs	0	False	476	Empty PDU
1357	10.732	Master	LE LL	0	22458µs	0	False	477	Empty PDU
1358	10.732	Slave	LE LL	0	150µs	0	False	477	Empty PDU
1359	10.755	Master	LE LL	0	22262µs	1	False	478	Empty PDU
1360	10.755	Slave	LE LL	0	150µs	1	False	478	Empty PDU
1361	10.777	Master	LE LL	0	22261µs	0	False	479	Empty PDU
1362	10.777	Slave	LE LL	0	150µs	0	False	479	Empty PDU
1363	10.800	Master	LE LL	0	22263µs	1	False	480	Empty PDU
1364	10.800	Slave	LE LL	0	150µs	1	False	480	Empty PDU
1365	10.822	Master	LE LL	0	22262µs	0	False	481	Empty PDU
1366	10.822	Slave	LE LL	0	150µs	0	False	481	Empty PDU
1367	10.845	Master	LE LL	0	22261µs	1	False	482	Empty PDU
1368	10.867	Master	LE LL	0	22457µs	1	False	483	Empty PDU
1369	10.890	Master	LE LL	0	22455µs	1	False	484	Empty PDU
1370	10.890	Slave	LE LL	0	150µs	1	False	484	Empty PDU
1371	10.912	Master	LE LL	0	22263µs	0	False	485	Empty PDU
1372	10.935	Master	LE LL	0	22457µs	0	False	486	Empty PDU
1373	10.957	Master	LE LL	0	22457µs	0	False	487	Empty PDU
1374	10.957	Slave	LE LL	0	150µs	0	False	487	Empty PDU
1375	10.980	Master	LE LL	0	22262µs	1	False	488	Empty PDU
1376	10.980	Slave	LE LL	0	150µs	1	False	488	Empty PDU
1377	11.002	Master	LE LL	0	22262µs	0	False	489	Empty PDU
1378	11.002	Slave	LE LL	0	150µs	0	False	489	Empty PDU
1379	11.025	Master	LE LL	0	22261µs	1	False	490	Empty PDU
1380	11.025	Slave	LE LL	0	150µs	1	False	490	Empty PDU
1381	11.047	Master	LE LL	0	22264µs	0	False	491	Empty PDU
1382	11.047	Slave	LE LL	0	150µs	0	False	491	Empty PDU
1383	11.070	Master	LE LL	0	22262µs	1	False	492	Empty PDU

1384	11.070	Slave	LE LL	0	150µs	1	False	492	Empty PDU
1385	11.092	Master	LE LL	0	22262µs	0	False	493	Empty PDU
1386	11.115	Master	LE LL	0	22457µs	0	False	494	Empty PDU
1387	11.137	Master	LE LL	0	22456µs	0	False	495	Empty PDU
1388	11.137	Slave	LE LL	0	150µs	0	False	495	Empty PDU
1389	11.160	Master	LE LL	0	22262µs	1	False	496	Empty PDU
1390	11.182	Master	LE LL	0	22456µs	1	False	497	Empty PDU
1391	11.205	Master	LE LL	0	22457µs	1	False	498	Empty PDU
1392	11.205	Slave	LE LL	0	149µs	1	False	498	Empty PDU
1393	11.227	Master	LE LL	0	22263µs	0	False	499	Empty PDU
1394	11.227	Slave	LE LL	0	150µs	0	False	499	Empty PDU
1395	11.250	Master	LE LL	0	22262µs	1	False	500	Empty PDU
1396	11.250	Slave	LE LL	0	150µs	1	False	500	Empty PDU
1397	11.272	Master	LE LL	0	22261µs	0	False	501	Empty PDU
1398	11.272	Slave	LE LL	0	150µs	0	False	501	Empty PDU
1399	11.295	Master	LE LL	0	22263µs	1	False	502	Empty PDU
1400	11.295	Slave	LE LL	0	150µs	1	False	502	Empty PDU
1401	11.317	Master	LE LL	0	22262µs	0	False	503	Empty PDU
1402	11.317	Slave	LE LL	0	150µs	0	False	503	Empty PDU
1403	11.340	Master	LE LL	0	22262µs	1	False	504	Empty PDU
1404	11.362	Master	LE LL	0	22456µs	1	False	505	Empty PDU
1405	11.385	Master	LE LL	0	22456µs	1	False	506	Empty PDU
1406	11.385	Slave	ATT	10	150µs	1	True	506	Rcvd Handle Value Indication, Handle: 0x000e (ZigBee Alliance: Unknown)
1407	11.385	Master	LE LL	0	150µs	0	False	506	Empty PDU
1408	11.385	Slave	LE LL	0	150µs	0	False	506	Empty PDU
1409	11.407	Master	ATT	5	21834µs	1	False	507	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
1410	11.430	Master	ATT	5	22435µs	1	False	508	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
1411	11.452	Master	ATT	5	22437µs	1	False	509	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
1412	11.452	Slave	LE LL	0	151µs	1	False	509	Empty PDU
1413	11.475	Master	LE LL	0	22241µs	0	False	510	Empty PDU
1414	11.475	Slave	LE LL	0	150µs	0	False	510	Empty PDU
1415	11.497	Master	LE LL	0	22262µs	1	False	511	Empty PDU
1416	11.497	Slave	LE LL	0	151µs	1	False	511	Empty PDU
1417	11.520	Master	LE LL	0	22262µs	0	False	512	Empty PDU
1418	11.520	Slave	LE LL	0	149µs	0	False	512	Empty PDU
1419	11.542	Master	LE LL	0	22263µs	1	False	513	Empty PDU
1420	11.542	Slave	LE LL	0	150µs	1	False	513	Empty PDU
1421	11.565	Master	LE LL	0	22263µs	0	False	514	Empty PDU
1422	11.565	Slave	LE LL	0	150µs	0	False	514	Empty PDU
1423	11.587	Master	LE LL	0	22263µs	1	False	515	Empty PDU
1424	11.587	Slave	LE LL	0	150µs	1	False	515	Empty PDU
1425	11.610	Master	LE LL	0	22261µs	0	False	516	Empty PDU
1426	11.610	Slave	LE LL	0	150µs	0	False	516	Empty PDU
1427	11.632	Master	LE LL	0	22264µs	1	False	517	Empty PDU
1428	11.632	Slave	LE LL	0	150µs	1	False	517	Empty PDU

1429	11.655	Master	LE LL	0	22262µs	0	False	518	Empty PDU
1430	11.655	Slave	LE LL	0	150µs	0	False	518	Empty PDU
1431	11.677	Master	LE LL	0	22261µs	1	False	519	Empty PDU
1432	11.677	Slave	LE LL	0	150µs	1	False	519	Empty PDU
1433	11.700	Master	LE LL	0	22262µs	0	False	520	Empty PDU
1434	11.700	Slave	LE LL	0	150µs	0	False	520	Empty PDU
1435	11.722	Master	LE LL	0	22264µs	1	False	521	Empty PDU
1436	11.722	Slave	LE LL	0	150µs	1	False	521	Empty PDU
1437	11.745	Master	LE LL	0	22262µs	0	False	522	Empty PDU
1438	11.745	Slave	LE LL	0	150µs	0	False	522	Empty PDU
1439	11.767	Master	LE LL	0	22262µs	1	False	523	Empty PDU
1440	11.767	Slave	LE LL	0	150µs	1	False	523	Empty PDU
1441	11.790	Master	LE LL	0	22263µs	0	False	524	Empty PDU
1442	11.790	Slave	LE LL	0	150µs	0	False	524	Empty PDU
1443	11.812	Master	LE LL	0	22262µs	1	False	525	Empty PDU
1444	11.812	Slave	LE LL	0	150µs	1	False	525	Empty PDU
1445	11.835	Master	LE LL	0	22262µs	0	False	526	Empty PDU
1446	11.835	Slave	LE LL	0	150µs	0	False	526	Empty PDU
1447	11.857	Master	LE LL	0	22263µs	1	False	527	Empty PDU
1448	11.857	Slave	LE LL	0	150µs	1	False	527	Empty PDU
1449	11.880	Master	LE LL	0	22262µs	0	False	528	Empty PDU
1450	11.880	Slave	LE LL	0	150µs	0	False	528	Empty PDU
1451	11.902	Master	LE LL	0	22263µs	1	False	529	Empty PDU
1452	11.902	Slave	LE LL	0	149µs	1	False	529	Empty PDU
1453	11.925	Master	LE LL	0	22263µs	0	False	530	Empty PDU
1454	11.925	Slave	LE LL	0	150µs	0	False	530	Empty PDU
1455	11.947	Master	LE LL	0	22263µs	1	False	531	Empty PDU
1456	11.947	Slave	LE LL	0	150µs	1	False	531	Empty PDU
1457	11.970	Master	LE LL	0	22263µs	0	False	532	Empty PDU
1458	11.970	Slave	LE LL	0	150µs	0	False	532	Empty PDU
1459	11.992	Master	LE LL	0	22261µs	1	False	533	Empty PDU
1460	11.992	Slave	LE LL	0	150µs	1	False	533	Empty PDU
1461	12.015	Master	LE LL	0	22262µs	0	False	534	Empty PDU
1462	12.015	Slave	LE LL	0	150µs	0	False	534	Empty PDU
1463	12.037	Master	LE LL	0	22264µs	1	False	535	Empty PDU
1464	12.037	Slave	LE LL	0	149µs	1	False	535	Empty PDU
1465	12.060	Master	LE LL	0	22262µs	0	False	536	Empty PDU
1466	12.060	Slave	LE LL	0	150µs	0	False	536	Empty PDU
1467	12.082	Master	LE LL	0	22263µs	1	False	537	Empty PDU
1468	12.082	Slave	LE LL	0	150µs	1	False	537	Empty PDU
1469	12.105	Master	LE LL	0	22262µs	0	False	538	Empty PDU
1470	12.105	Slave	LE LL	0	150µs	0	False	538	Empty PDU
1471	12.127	Master	LE LL	0	22263µs	1	False	539	Empty PDU
1472	12.127	Slave	LE LL	0	150µs	1	False	539	Empty PDU
1473	12.150	Master	LE LL	0	22262µs	0	False	540	Empty PDU

1474	12.150	Slave	LE LL	0	150µs	0	False	540	Empty PDU
1475	12.172	Master	LE LL	0	22263µs	1	False	541	Empty PDU
1476	12.172	Slave	LE LL	0	149µs	1	False	541	Empty PDU
1477	12.195	Master	LE LL	0	22261µs	0	False	542	Empty PDU
1478	12.195	Slave	LE LL	0	150µs	0	False	542	Empty PDU
1479	12.217	Master	LE LL	0	22262µs	1	False	543	Empty PDU
1480	12.217	Slave	LE LL	0	150µs	1	False	543	Empty PDU
1481	12.240	Master	LE LL	0	22263µs	0	False	544	Empty PDU
1482	12.240	Slave	LE LL	0	150µs	0	False	544	Empty PDU
1483	12.262	Master	LE LL	0	22262µs	1	False	545	Empty PDU
1484	12.262	Slave	LE LL	0	150µs	1	False	545	Empty PDU
1485	12.285	Master	LE LL	0	22262µs	0	False	546	Empty PDU
1486	12.285	Slave	LE LL	0	150µs	0	False	546	Empty PDU
1487	12.307	Master	LE LL	0	22263µs	1	False	547	Empty PDU
1488	12.307	Slave	LE LL	0	150µs	1	False	547	Empty PDU
1489	12.330	Master	LE LL	0	22263µs	0	False	548	Empty PDU
1490	12.352	Master	LE LL	0	22455µs	0	False	549	Empty PDU
1491	12.375	Master	LE LL	0	22458µs	0	False	550	Empty PDU
1492	12.375	Slave	LE LL	0	150µs	0	False	550	Empty PDU
1493	12.397	Master	LE LL	0	22261µs	1	False	551	Empty PDU
1494	12.420	Master	LE LL	0	22456µs	1	False	552	Empty PDU
1495	12.442	Master	LE LL	0	22456µs	1	False	553	Empty PDU
1496	12.442	Slave	LE LL	0	150µs	1	False	553	Empty PDU
1497	12.465	Master	LE LL	0	22264µs	0	False	554	Empty PDU
1498	12.465	Slave	LE LL	0	150µs	0	False	554	Empty PDU
1499	12.487	Master	LE LL	0	22262µs	1	False	555	Empty PDU
1500	12.487	Slave	LE LL	27	150µs	1	True	555	L2CAP Fragment Start
1501	12.488	Master	LE LL	0	150µs	0	False	555	Empty PDU
1502	12.488	Slave	LE LL	27	150µs	0	True	555	L2CAP Fragment
1503	12.488	Master	LE LL	0	150µs	1	False	555	Empty PDU
1504	12.488	Slave	LE LL	22	150µs	1	True	555	L2CAP Fragment
1505	12.489	Master	LE LL	0	150µs	0	False	555	Empty PDU
1506	12.510	Master	LE LL	0	20988µs	0	True	556	Empty PDU
1507	12.532	Master	LE LL	0	22456µs	0	True	557	Empty PDU
1508	12.555	Master	LE LL	0	22456µs	0	True	558	Empty PDU
1509	12.555	Slave	LE LL	0	150µs	0	False	558	Empty PDU
1510	12.555	Master	ATT	5	150µs	1	False	558	Sent Handle Value Confirmation, Handle: 0x000e (ZigBee Alliance: Unknown)
1511	12.555	Slave	LE LL	0	150µs	1	False	558	Empty PDU
1512	12.577	Master	LE LL	0	21853µs	0	False	559	Empty PDU
1513	12.577	Slave	LE LL	0	150µs	0	False	559	Empty PDU
1514	12.600	Master	LE LL	0	22263µs	1	False	560	Empty PDU
1515	12.600	Slave	LE LL	0	150µs	1	False	560	Empty PDU
1516	12.622	Master	LE LL	0	22263µs	0	False	561	Empty PDU
1517	12.622	Slave	LE LL	0	149µs	0	False	561	Empty PDU
1518	12.645	Master	LE LL	0	22262µs	1	False	562	Empty PDU

1519	12.645	Slave	LE LL	0	150µs	1	False	562	Empty PDU
1520	12.667	Master	LE LL	0	22262µs	0	False	563	Empty PDU
1521	12.667	Slave	LE LL	0	150µs	0	False	563	Empty PDU
1522	12.690	Master	LE LL	0	22262µs	1	False	564	Empty PDU
1523	12.690	Slave	LE LL	0	151µs	1	False	564	Empty PDU
1524	12.712	Master	LE LL	0	22262µs	0	False	565	Empty PDU
1525	12.712	Slave	LE LL	0	150µs	0	False	565	Empty PDU
1526	12.735	Master	LE LL	0	22262µs	1	False	566	Empty PDU
1527	12.735	Slave	LE LL	0	150µs	1	False	566	Empty PDU
1528	12.757	Master	LE LL	0	22262µs	0	False	567	Empty PDU
1529	12.757	Slave	LE LL	0	150µs	0	False	567	Empty PDU
1530	12.780	Master	LE LL	0	22262µs	1	False	568	Empty PDU
1531	12.780	Slave	LE LL	0	150µs	1	False	568	Empty PDU
1532	12.802	Master	LE LL	0	22263µs	0	False	569	Empty PDU
1533	12.825	Master	LE LL	0	22455µs	0	False	570	Empty PDU
1534	12.825	Slave	LE LL	0	150µs	0	False	570	Empty PDU
1535	12.847	Master	LE LL	0	22261µs	1	False	571	Empty PDU
1536	12.847	Slave	LE LL	0	150µs	1	False	571	Empty PDU
1537	12.870	Master	LE LL	0	22264µs	0	False	572	Empty PDU
1538	12.870	Slave	LE LL	0	150µs	0	False	572	Empty PDU
1539	12.892	Master	LE LL	0	22262µs	1	False	573	Empty PDU
1540	12.892	Slave	LE LL	0	150µs	1	False	573	Empty PDU
1541	12.915	Master	LE LL	0	22262µs	0	False	574	Empty PDU
1542	12.937	Master	LE LL	0	22456µs	0	False	575	Empty PDU
1543	12.960	Master	LE LL	0	22456µs	0	False	576	Empty PDU
1544	12.960	Slave	LE LL	0	150µs	0	False	576	Empty PDU
1545	12.982	Master	LE LL	0	22262µs	1	False	577	Empty PDU
1546	12.982	Slave	LE LL	0	150µs	1	False	577	Empty PDU
1547	13.005	Master	LE LL	0	22262µs	0	False	578	Empty PDU
1548	13.027	Master	LE LL	0	22456µs	0	False	579	Empty PDU
1549	13.050	Master	LE LL	0	22458µs	0	False	580	Empty PDU
1550	13.050	Slave	LE LL	0	150µs	0	False	580	Empty PDU
1551	13.072	Master	LE LL	0	22261µs	1	False	581	Empty PDU
1552	13.072	Slave	LE LL	0	150µs	1	False	581	Empty PDU
1553	13.095	Master	LE LL	0	22263µs	0	False	582	Empty PDU
1554	13.095	Slave	LE LL	0	149µs	0	False	582	Empty PDU
1555	13.117	Master	LE LL	0	22262µs	1	False	583	Empty PDU
1556	13.117	Slave	LE LL	0	150µs	1	False	583	Empty PDU
1557	13.140	Master	LE LL	0	22262µs	0	False	584	Empty PDU
1558	13.140	Slave	LE LL	0	150µs	0	False	584	Empty PDU
1559	13.162	Master	LE LL	0	22264µs	1	False	585	Empty PDU
1560	13.162	Slave	LE LL	0	150µs	1	False	585	Empty PDU
1561	13.185	Master	LE LL	0	22262µs	0	False	586	Empty PDU
1562	13.185	Slave	LE LL	0	150µs	0	False	586	Empty PDU
1563	13.207	Master	LE LL	0	22263µs	1	False	587	Empty PDU

1564	13.230	Master	LE LL	0	22456µs	1	False	588	Empty PDU
1565	13.252	Master	LE LL	0	22455µs	1	False	589	Empty PDU
1566	13.252	Slave	LE LL	0	151µs	1	False	589	Empty PDU
1567	13.275	Master	LE LL	0	22261µs	0	False	590	Empty PDU
1568	13.275	Slave	LE LL	0	150µs	0	False	590	Empty PDU
1569	13.297	Master	LE LL	0	22262µs	1	False	591	Empty PDU
1570	13.297	Slave	LE LL	0	150µs	1	False	591	Empty PDU
1571	13.320	Master	LE LL	0	22262µs	0	False	592	Empty PDU
1572	13.320	Slave	LE LL	0	150µs	0	False	592	Empty PDU
1573	13.342	Master	LE LL	0	22262µs	1	False	593	Empty PDU
1574	13.342	Slave	LE LL	0	150µs	1	False	593	Empty PDU
1575	13.365	Master	LE LL	0	22262µs	0	False	594	Empty PDU
1576	13.365	Slave	LE LL	0	150µs	0	False	594	Empty PDU
1577	13.387	Master	LE LL	0	22264µs	1	False	595	Empty PDU
1578	13.387	Slave	LE LL	0	150µs	1	False	595	Empty PDU
1579	13.410	Master	LE LL	0	22259µs	0	False	596	Empty PDU
1580	13.410	Slave	LE LL	0	150µs	0	False	596	Empty PDU
1581	13.432	Master	LE LL	0	22262µs	1	False	597	Empty PDU
1582	13.455	Master	LE LL	0	22458µs	1	False	598	Empty PDU
1583	13.477	Master	LE LL	0	22455µs	1	False	599	Empty PDU
1584	13.477	Slave	LE LL	0	150µs	1	False	599	Empty PDU
1585	13.500	Master	LE LL	0	22261µs	0	False	600	Empty PDU
1586	13.500	Slave	LE LL	0	150µs	0	False	600	Empty PDU
1587	13.522	Master	LE LL	0	22263µs	1	False	601	Empty PDU
1588	13.545	Master	LE LL	0	22457µs	1	False	602	Empty PDU
1589	13.567	Master	LE LL	0	22456µs	1	False	603	Empty PDU
1590	13.567	Slave	LE LL	0	150µs	1	False	603	Empty PDU
1591	13.590	Master	LE LL	0	22262µs	0	False	604	Empty PDU
1592	13.590	Slave	LE LL	0	150µs	0	False	604	Empty PDU
1593	13.612	Master	LE LL	0	22262µs	1	False	605	Empty PDU
1594	13.612	Slave	LE LL	0	150µs	1	False	605	Empty PDU
1595	13.635	Master	LE LL	0	22263µs	0	False	606	Empty PDU
1596	13.657	Master	LE LL	0	22456µs	0	False	607	Empty PDU
1597	13.680	Master	LE LL	0	22456µs	0	False	608	Empty PDU
1598	13.680	Slave	LE LL	0	150µs	0	False	608	Empty PDU
1599	13.702	Master	LE LL	0	22261µs	1	False	609	Empty PDU
1600	13.702	Slave	LE LL	0	150µs	1	False	609	Empty PDU
1601	13.725	Master	LE LL	0	22262µs	0	False	610	Empty PDU
1602	13.747	Master	LE LL	0	22458µs	0	False	611	Empty PDU
1603	13.770	Master	LE LL	0	22457µs	0	False	612	Empty PDU
1604	13.770	Slave	LE LL	0	150µs	0	False	612	Empty PDU
1605	13.792	Master	LE LL	0	22262µs	1	False	613	Empty PDU
1606	13.792	Slave	LE LL	0	150µs	1	False	613	Empty PDU
1607	13.815	Master	LE LL	0	22263µs	0	False	614	Empty PDU
1608	13.815	Slave	LE LL	0	150µs	0	False	614	Empty PDU

1609	13.837	Master	LE LL	0	22261µs	1	False	615	Empty PDU
1610	13.860	Master	LE LL	0	22456µs	1	False	616	Empty PDU
1611	13.882	Master	LE LL	0	22457µs	1	False	617	Empty PDU
1612	13.882	Slave	LE LL	0	150µs	1	False	617	Empty PDU
1613	13.905	Master	ATT	10	22262µs	0	False	618	Sent Write Request, Handle: 0x000c (ZigBee Alliance: Unknown)
1614	13.905	Slave	LE LL	0	150µs	0	False	618	Empty PDU
1615	13.927	Master	LE LL	0	22222µs	1	False	619	Empty PDU
1616	13.950	Master	LE LL	0	22455µs	1	False	620	Empty PDU
1617	13.972	Master	LE LL	0	22456µs	1	False	621	Empty PDU
1618	13.972	Slave	ATT	5	151µs	1	True	621	Rcvd Write Response, Handle: 0x000c (ZigBee Alliance: Unknown)
1619	13.973	Master	LE LL	0	149µs	0	False	621	Empty PDU
1620	13.973	Slave	LE LL	0	151µs	0	False	621	Empty PDU
1621	13.995	Master	LE LL	0	21855µs	1	False	622	Empty PDU
1622	13.995	Slave	LE LL	0	150µs	1	False	622	Empty PDU
1623	14.017	Master	LE LL	0	22260µs	0	False	623	Empty PDU
1624	14.017	Slave	LE LL	0	150µs	0	False	623	Empty PDU
1625	14.040	Master	LE LL	0	22262µs	1	False	624	Empty PDU
1626	14.040	Slave	LE LL	0	150µs	1	False	624	Empty PDU
1627	14.062	Master	LE LL	0	22263µs	0	False	625	Empty PDU
1628	14.062	Slave	LE LL	0	150µs	0	False	625	Empty PDU
1629	14.085	Master	LE LL	0	22262µs	1	False	626	Empty PDU
1630	14.085	Slave	LE LL	0	150µs	1	False	626	Empty PDU
1631	14.107	Master	LE LL	0	22262µs	0	False	627	Empty PDU
1632	14.107	Slave	LE LL	0	150µs	0	False	627	Empty PDU
1633	14.130	Master	LE LL	0	22262µs	1	False	628	Empty PDU
1634	14.152	Master	LE LL	0	22456µs	1	False	629	Empty PDU
1635	14.175	Master	LE LL	0	22457µs	1	False	630	Empty PDU
1636	14.175	Slave	LE LL	0	151µs	1	False	630	Empty PDU
1637	14.197	Master	LE LL	0	22261µs	0	False	631	Empty PDU
1638	14.197	Slave	LE LL	0	149µs	0	False	631	Empty PDU
1639	14.220	Master	LE LL	0	22263µs	1	False	632	Empty PDU
1640	14.220	Slave	LE LL	0	150µs	1	False	632	Empty PDU
1641	14.242	Master	LE LL	0	22262µs	0	False	633	Empty PDU
1642	14.265	Master	LE LL	0	22456µs	0	False	634	Empty PDU
1643	14.287	Master	LE LL	0	22456µs	0	False	635	Empty PDU
1644	14.287	Slave	LE LL	0	150µs	0	False	635	Empty PDU
1645	14.310	Master	LE LL	0	22263µs	1	False	636	Empty PDU
1646	14.310	Slave	LE LL	0	150µs	1	False	636	Empty PDU
1647	14.332	Master	LE LL	0	22263µs	0	False	637	Empty PDU
1648	14.355	Master	LE LL	0	22456µs	0	False	638	Empty PDU
1649	14.377	Master	LE LL	0	22456µs	0	False	639	Empty PDU
1650	14.377	Slave	LE LL	0	151µs	0	False	639	Empty PDU
1651	14.400	Master	LE LL	0	22261µs	1	False	640	Empty PDU
1652	14.400	Slave	LE LL	0	150µs	1	False	640	Empty PDU
1653	14.422	Master	LE LL	0	22262µs	0	False	641	Empty PDU

1654	14.422	Slave	LE LL	0	150µs	0	False	641	Empty PDU
1655	14.445	Master	LE LL	0	22263µs	1	False	642	Empty PDU
1656	14.467	Master	LE LL	0	22455µs	1	False	643	Empty PDU
1657	14.490	Master	LE LL	0	22458µs	1	False	644	Empty PDU
1658	14.490	Slave	LE LL	0	151µs	1	False	644	Empty PDU
1659	14.512	Master	LE LL	0	22262µs	0	False	645	Empty PDU
1660	14.512	Slave	LE LL	0	149µs	0	False	645	Empty PDU
1661	14.535	Master	LE LL	0	22262µs	1	False	646	Empty PDU
1662	14.535	Slave	LE LL	0	150µs	1	False	646	Empty PDU
1663	14.557	Master	LE LL	0	22262µs	0	False	647	Empty PDU
1664	14.580	Master	LE LL	0	22456µs	0	False	648	Empty PDU
1665	14.602	Master	LE LL	0	22457µs	0	False	649	Empty PDU
1666	14.602	Slave	LE LL	0	150µs	0	False	649	Empty PDU
1667	14.625	Master	LE LL	0	22262µs	1	False	650	Empty PDU
1668	14.625	Slave	LE LL	0	150µs	1	False	650	Empty PDU
1669	14.647	Master	LE LL	0	22262µs	0	False	651	Empty PDU
1670	14.670	Master	LE LL	0	22456µs	0	False	652	Empty PDU
1671	14.692	Master	LE LL	0	22457µs	0	False	653	Empty PDU
1672	14.692	Slave	LE LL	0	150µs	0	False	653	Empty PDU
1673	14.715	Master	LE LL	0	22263µs	1	False	654	Empty PDU
1674	14.715	Slave	LE LL	0	150µs	1	False	654	Empty PDU
1675	14.737	Master	LE LL	0	22262µs	0	False	655	Empty PDU
1676	14.737	Slave	LE LL	0	150µs	0	False	655	Empty PDU
1677	14.760	Master	LE LL	0	22261µs	1	False	656	Empty PDU
1678	14.782	Master	LE LL	0	22456µs	1	False	657	Empty PDU
1679	14.805	Master	LE LL	0	22457µs	1	False	658	Empty PDU
1680	14.805	Slave	LE LL	0	150µs	1	False	658	Empty PDU
1681	14.827	Master	LE LL	0	22262µs	0	False	659	Empty PDU
1682	14.827	Slave	LE LL	0	150µs	0	False	659	Empty PDU
1683	14.850	Master	LE LL	0	22261µs	1	False	660	Empty PDU
1684	14.872	Master	LE LL	0	22456µs	1	False	661	Empty PDU
1685	14.872	Slave	LE LL	0	150µs	1	False	661	Empty PDU
1686	14.895	Master	LE LL	0	22264µs	0	False	662	Empty PDU
1687	14.895	Slave	LE LL	0	150µs	0	False	662	Empty PDU
1688	14.917	Master	LE LL	0	22261µs	1	False	663	Empty PDU
1689	14.917	Slave	LE LL	0	150µs	1	False	663	Empty PDU
1690	14.940	Master	LE LL	0	22262µs	0	False	664	Empty PDU
1691	14.940	Slave	LE LL	0	150µs	0	False	664	Empty PDU
1692	14.962	Master	LE LL	0	22263µs	1	False	665	Empty PDU
1693	14.962	Slave	LE LL	0	150µs	1	False	665	Empty PDU
1694	14.985	Master	LE LL	0	22261µs	0	False	666	Empty PDU
1695	14.985	Slave	LE LL	0	150µs	0	False	666	Empty PDU
1696	15.007	Master	LE LL	0	22263µs	1	False	667	Empty PDU
1697	15.007	Slave	LE LL	0	149µs	1	False	667	Empty PDU
1698	15.030	Master	LE LL	0	22263µs	0	False	668	Empty PDU

1699	15.030	Slave	LE LL	0	150µs	0	False	668	Empty PDU
1700	15.052	Master	LE LL	0	22262µs	1	False	669	Empty PDU
1701	15.075	Master	LE LL	0	22456µs	1	False	670	Empty PDU
1702	15.075	Slave	LE LL	0	150µs	1	False	670	Empty PDU
1703	15.097	Master	LE LL	0	22262µs	0	False	671	Empty PDU
1704	15.097	Slave	LE LL	0	150µs	0	False	671	Empty PDU
1705	15.120	Master	LE LL	0	22263µs	1	False	672	Empty PDU
1706	15.120	Slave	LE LL	0	150µs	1	False	672	Empty PDU
1707	15.142	Master	LE LL	0	22263µs	0	False	673	Empty PDU
1708	15.142	Slave	LE LL	0	150µs	0	False	673	Empty PDU
1709	15.165	Master	LE LL	0	22261µs	1	False	674	Empty PDU
1710	15.187	Master	LE LL	0	22456µs	1	False	675	Empty PDU
1711	15.210	Master	LE LL	0	22457µs	1	False	676	Empty PDU
1712	15.210	Slave	LE LL	0	150µs	1	False	676	Empty PDU
1713	15.232	Master	LE LL	0	22262µs	0	False	677	Empty PDU
1714	15.232	Slave	LE LL	0	150µs	0	False	677	Empty PDU
1715	15.255	Master	LE LL	0	22262µs	1	False	678	Empty PDU
1716	15.277	Master	LE LL	0	22456µs	1	False	679	Empty PDU
1717	15.300	Master	LE LL	0	22457µs	1	False	680	Empty PDU
1718	15.300	Slave	LE LL	0	151µs	1	False	680	Empty PDU
1719	15.322	Master	LE LL	0	22262µs	0	False	681	Empty PDU
1720	15.322	Slave	LE LL	0	150µs	0	False	681	Empty PDU
1721	15.345	Master	LE LL	0	22261µs	1	False	682	Empty PDU
1722	15.345	Slave	LE LL	0	150µs	1	False	682	Empty PDU
1723	15.367	Master	LE LL	0	22262µs	0	False	683	Empty PDU
1724	15.367	Slave	LE LL	0	150µs	0	False	683	Empty PDU
1725	15.390	Master	LE LL	0	22264µs	1	False	684	Empty PDU
1726	15.390	Slave	LE LL	0	150µs	1	False	684	Empty PDU
1727	15.412	Master	LE LL	0	22262µs	0	False	685	Empty PDU
1728	15.412	Slave	LE LL	0	150µs	0	False	685	Empty PDU
1729	15.435	Master	LE LL	0	22262µs	1	False	686	Empty PDU
1730	15.435	Slave	LE LL	0	150µs	1	False	686	Empty PDU
1731	15.457	Master	LE LL	0	22262µs	0	False	687	Empty PDU
1732	15.457	Slave	LE LL	0	150µs	0	False	687	Empty PDU
1733	15.480	Master	LE LL	0	22262µs	1	False	688	Empty PDU
1734	15.502	Master	LE LL	0	22458µs	1	False	689	Empty PDU
1735	15.525	Master	LE LL	0	22455µs	1	False	690	Empty PDU
1736	15.525	Slave	LE LL	0	149µs	1	False	690	Empty PDU
1737	15.547	Master	LE LL	0	22264µs	0	False	691	Empty PDU
1738	15.547	Slave	LE LL	0	150µs	0	False	691	Empty PDU
1739	15.570	Master	LE LL	0	22262µs	1	False	692	Empty PDU
1740	15.592	Master	LE LL	0	22457µs	1	False	693	Empty PDU
1741	15.615	Master	LE LL	0	22456µs	1	False	694	Empty PDU
1742	15.615	Slave	LE LL	0	150µs	1	False	694	Empty PDU
1743	15.637	Master	LE LL	0	22261µs	0	False	695	Empty PDU

1744	15.637	Slave	LE LL	0	150µs	0	False	695	Empty PDU
1745	15.660	Master	LE LL	0	22264µs	1	False	696	Empty PDU
1746	15.660	Slave	LE LL	0	149µs	1	False	696	Empty PDU
1747	15.682	Master	LE LL	0	22261µs	0	False	697	Empty PDU
1748	15.705	Master	LE LL	0	22457µs	0	False	698	Empty PDU
1749	15.727	Master	LE LL	0	22457µs	0	False	699	Empty PDU
1750	15.727	Slave	LE LL	0	150µs	0	False	699	Empty PDU
1751	15.750	Master	LE LL	0	22261µs	1	False	700	Empty PDU
1752	15.750	Slave	LE LL	0	150µs	1	False	700	Empty PDU
1753	15.772	Master	LE LL	0	22262µs	0	False	701	Empty PDU
1754	15.795	Master	LE LL	0	22457µs	0	False	702	Empty PDU
1755	15.817	Master	LE LL	0	22456µs	0	False	703	Empty PDU
1756	15.817	Slave	LE LL	0	150µs	0	False	703	Empty PDU
1757	15.840	Master	LE LL	2	22262µs	1	True	704	Control Opcode: LL_TERMINATE_IND
1758	15.840	Slave	LE LL	0	150µs	1	False	704	Empty PDU
1759	15.840	Master	L2CAP	9	150µs	0	False	704	Connection oriented channel
1760	15.840	Slave	LE LL	0	150µs	1	False	704	Empty PDU

5. De-authentication of the test network, AP attacked

```
michael@michael-Aspire-V7-582PG:~$ iwconfig
lo        no wireless extensions.

enp5s0f1  no wireless extensions.

wlp4s0    IEEE 802.11  ESSID:"Test Network"
          Mode:Managed  Frequency:2.437 GHz  Access Point: E2:26:26:89:69:DD
          Bit Rate=28.9 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=29/70  Signal level=-81 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:48   Missed beacon:0

michael@michael-Aspire-V7-582PG:~$ ping google.com
PING google.com(fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e)) 56 data bytes
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=1 ttl=113 time=72.1 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=2 ttl=113 time=244 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=3 ttl=113 time=83.9 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=4 ttl=113 time=292 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=5 ttl=113 time=32.8 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=6 ttl=113 time=82.1 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=7 ttl=113 time=121 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=8 ttl=113 time=497 ms
64 bytes from 2a00:1450:4001:82a::200e: icmp_seq=9 ttl=113 time=161 ms
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=10 Destination unreachable: Address unreachable
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=11 Destination unreachable: Address unreachable
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=12 Destination unreachable: Address unreachable
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=16 Destination unreachable: Address unreachable
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=17 Destination unreachable: Address unreachable
From michael-Aspire-V7-582PG (2a01:598:d84d:5c4e:c663:284e:63b6:4d2f) icmp_seq=18 Destination unreachable: Address unreachable
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=19 ttl=113 time=63.7 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=20 ttl=113 time=62.8 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=21 ttl=113 time=62.3 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=22 ttl=113 time=76.8 ms
64 bytes from fra24s07-in-x0e.1e100.net (2a00:1450:4001:82a::200e): icmp_seq=23 ttl=113 time=98.3 ms
^C
--- google.com ping statistics ---
23 packets transmitted, 14 received, +6 errors, 39.1304% packet loss, time 22227ms
rtt min/avg/max/mdev = 32.767/139.304/497.439/122.085 ms
michael@michael-Aspire-V7-582PG:~$
```

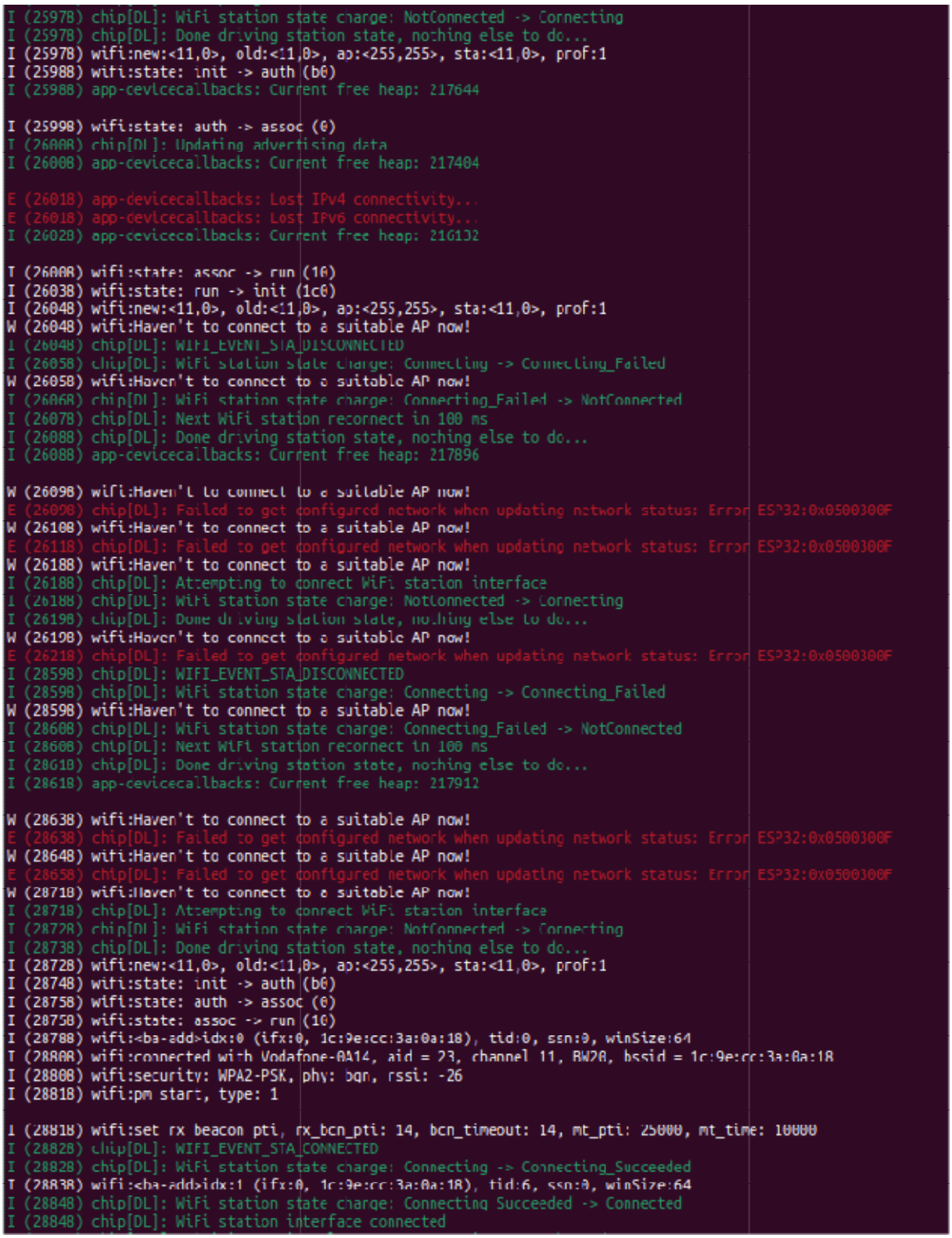
6. De-authentication of home router, computer attacked

```
michael@michael-Aspire-V7-582PG:~$ iwconfig
lo        no wireless extensions.

enp5s0f1  no wireless extensions.

wlp4s0    IEEE 802.11  ESSID:"Vodafone-0A14"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 1C:9E:CC:3A:0A:18
          Bit Rate=57.8 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=26/70  Signal level=-84 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:3   Missed beacon:0

michael@michael-Aspire-V7-582PG:~$ ping google.com
PING google.com(fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e)) 56 data bytes
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=1 ttl=118 time=12.9 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=2 ttl=118 time=10.3 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=3 ttl=118 time=11.3 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=4 ttl=118 time=12.0 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=5 ttl=118 time=10.6 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=6 ttl=118 time=14.3 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=7 ttl=118 time=10.3 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=8 ttl=118 time=12.0 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=9 ttl=118 time=12.5 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=10 ttl=118 time=9.52 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=11 ttl=118 time=11.2 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=12 ttl=118 time=10.8 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=13 ttl=118 time=9.49 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=14 ttl=118 time=10.0 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=15 ttl=118 time=9.52 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=16 ttl=118 time=9.44 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=17 ttl=118 time=11.9 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=18 ttl=118 time=13.0 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=19 ttl=118 time=12.7 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=20 ttl=118 time=11.0 ms
^C
--- google.com ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19029ms
rtt min/avg/max/mdev = 9.444/11.249/14.264/1.346 ms
michael@michael-Aspire-V7-582PG:~$
```

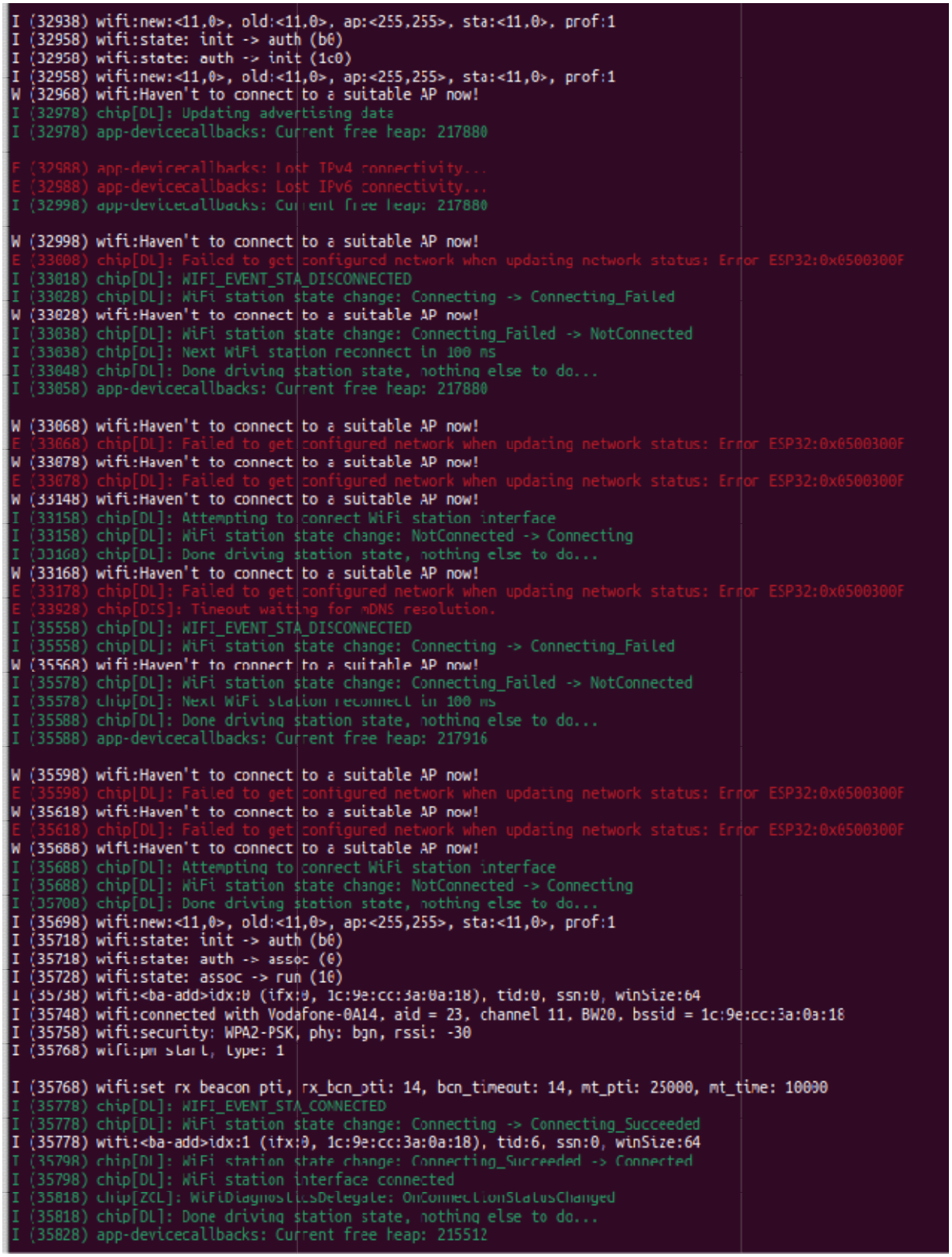
7. De-authentication of home router, AP attacked

```
michael@michael-Aspire-V7-582PG:~$ iwconfig
lo        no wireless extensions.

enp5s0f1  no wireless extensions.

wlp4s0    IEEE 802.11  ESSID:"Vodafone-0A14"
          Mode:Managed  Frequency:5.5 GHz  Access Point: 1C:9E:CC:3A:0A:20
          Bit Rate=240 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=44/70  Signal level=-66 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:47   Missed beacon:0

michael@michael-Aspire-V7-582PG:~$ ping google.com
PING google.com(fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e)) 56 data bytes
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=1 ttl=118 time=8.94 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=2 ttl=118 time=10.1 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=3 ttl=118 time=11.7 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=4 ttl=118 time=12.9 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=5 ttl=118 time=10.0 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=6 ttl=118 time=10.5 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=7 ttl=118 time=14.6 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=8 ttl=118 time=9.98 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=9 ttl=118 time=10.5 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=10 ttl=118 time=10.5 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=11 ttl=118 time=13.6 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=12 ttl=118 time=10.8 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=13 ttl=118 time=11.7 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=14 ttl=118 time=11.9 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=15 ttl=118 time=12.2 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=16 ttl=118 time=12.3 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=17 ttl=118 time=10.9 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=18 ttl=118 time=10.1 ms
64 bytes from fra16s48-in-x0e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=19 ttl=118 time=12.2 ms
64 bytes from fra07s63-in-x200e.1e100.net (2a00:1450:4001:80e::200e): icmp_seq=20 ttl=118 time=10.1 ms
^C
--- google.com ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19031ms
rtt min/avg/max/mdev = 8.939/11.282/14.646/1.374 ms
michael@michael-Aspire-V7-582PG:~$
```

8. De-authentication of Matter network, AP attacked



9. De-authentication of Matter network, Matter device attacked



10. Client-Server replay attack execution

```
michael@michael-Aspire-V7-582PG:~$ sudo python3 replaytest.py
###[ Ethernet ]###
  dst       = 30:de:4b:f4:bc:78
  src       = 0c:8b:fd:08:d7:de
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 58
     id        = 50749
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0xf277
     src       = 192.168.0.140
     dst       = 192.168.0.33
     \options   \
###[ UDP ]###
        sport     = 9999
        dport     = 43061
        len       = 38
        chksum    = 0x83f
###[ Raw ]###
           load      = 'Message from Server to Client\n'

###[ Ethernet ]###
  dst       = 30:de:4b:f4:bc:78
  src       = 0c:8b:fd:08:d7:de
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = None
     id        = 50749
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = None
     src       = 192.168.0.140
     dst       = 192.168.0.33
     \options   \
###[ UDP ]###
        sport     = 9999
        dport     = 43061
        len       = None
        chksum    = None
###[ Raw ]###
           load      = 'Message from Server to Client\n'

###[ Ethernet ]###
  dst       = 30:de:4b:f4:bc:78
  src       = 0c:8b:fd:08:d7:de
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 47
     id        = 50749
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0xf282
     src       = 192.168.0.140
     dst       = 192.168.0.33
     \options   \
###[ UDP ]###
        sport     = 9999
        dport     = 43061
        len       = 27
        chksum    = 0x760d
###[ Raw ]###
           load      = 'manipulated message'

.
Sent 1 packets.
michael@michael-Aspire-V7-582PG:~$
```