Технология 6LoWPAN. Стандарт IEEE 802.15.4

проф. д-р инж. Венета Алексиева

Основни моменти

- IEEE 802.15.4
- 6LoWPAN
- Хедъри
- Фрагментация
- Маршрутизиране
- Сигурност

История

- 2003г. излиза стандартът IEEE 802.15.4, който води до стандартизация на 6LoWPAN.
- 2007 г. излиза RFC 4919 за 6LoWPAN, който определя формата 6LoWPAN и неговата функционалност.
- През 2008 г. е създадена нова работна група на IETF, Routing over Low-power and Lossy Networks (ROLL). Задачата на тази работна група е да определи изискванията за маршрутизиране и разяснения или решения за мрежи с ниска мощност, безжични и нестабилни мрежи.
- 2008 г. ISA стартира стандартизация на безжична индустриална система за автоматизация, наречена SP100.11a (известна още като ISA100), която е базирана на 6LoWPAN.
- 2009 г. ETSI създава работна група за регулиране на M2M, която се състои от IP-архитектура от край до край, съвместима със 6LoWPAN.
- 2011г. Излиза RFC 6282 за компресирани формати за IPv6 върху IEEE 802.15.4
- 2012г. Излиза RFC 6775 за оптимизация при откриване на съседства за 6LoWPANs

Същност на 6loWPAN

- 6LoWPAN представлява адаптивен слой, който позволява IPv6 пакети да се предават ефективно в малки фреймове.
- 6LoWPAN е отворен стандарт, дефиниран в RFC 6282 и RFC 4919.
- 6LoWPAN е замислена да поддържа IEEE 802.15.4 за нискоенергийни безжични мрежи в 2.4GHz честотна лента.
- 6LoWPAN се адаптира и използва за различни други мрежови преносни среди:
  - Sub-1GHz low-power RF,
  - Bluetooth Smart,
  - Power Line Control (PLC)
  - Wi-Fi с ниска мощност.

Приложение на 6loWPAN

- контрол на състоянието на оборудването;
- следене състоянието на околната среда;
- реализиране на сигурност и защита;
- приложение в домашна среда;
- автоматизация на сгради.

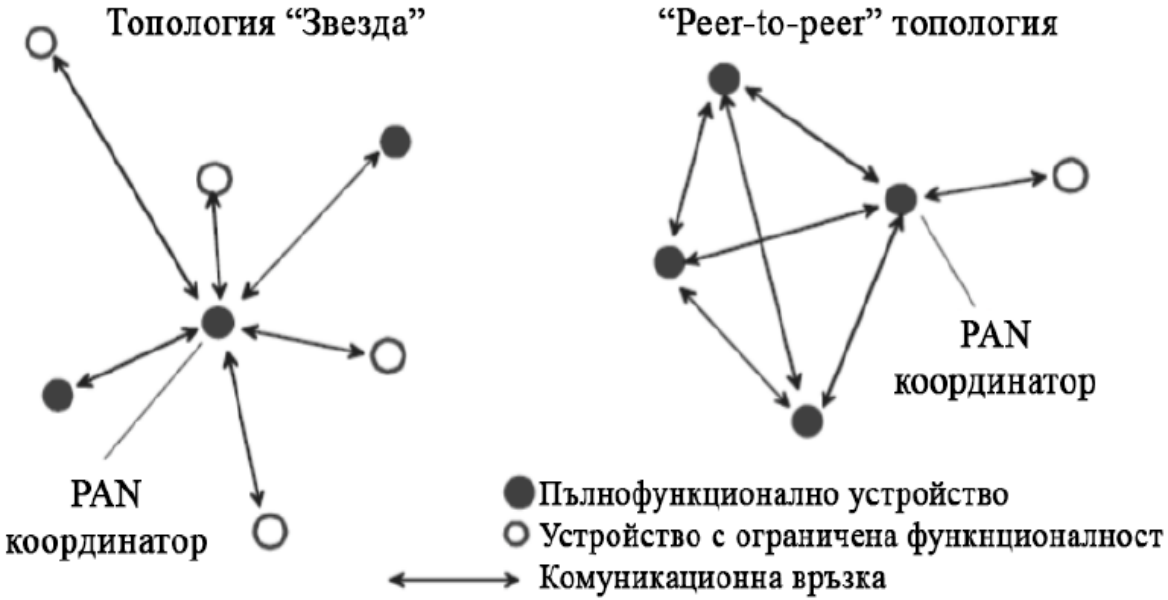
IEEE 802.15.4 стандарт

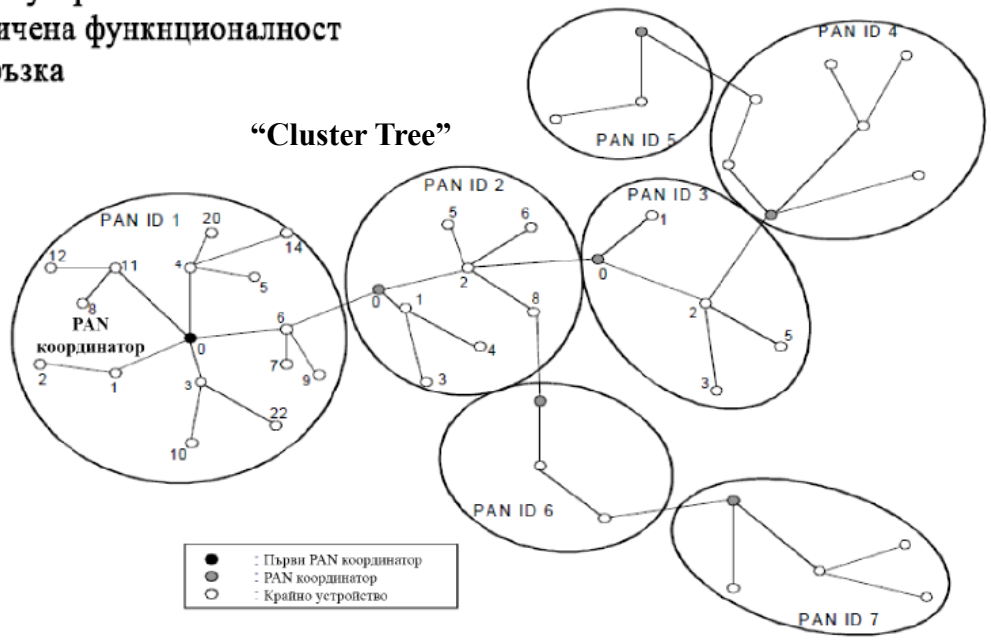
- IEEE 802.15.4 е технически стандарт, който дефинира оперирането на LR-WPANs в приложения с ограничена мощност и ниски изисквания за производителност.
- Основните цели на LR-WPANs са:
  - лесна инсталация,
  - надежден трансфер на данни,
  - изключително ниска цена
  - дълъг живот на батерията,
  - прост и гъвкав протокол, осигуряващ безжична връзка.

IEEE 802.15.4 устройства

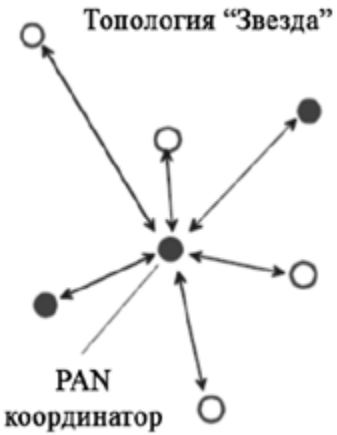
- FFD – Fully Functional Device;
  - способно е да обслужва PAN мрежата. Може да изпълнява ролята на PAN координатор, маршрутизатор, крайно устройство, RFD или като комбинация от тях и осъществява комуникация с всяко друго устройство в мрежата. Може да бъде използвано в каквато и да е топология;
- RFD – Reduced Functionality Device.
  - предназначено е за съвсем прости приложения (ключ за лампа, пасивен инфрачервен сензор). Не изпраща големи количества информация и се асоциира само с едно пълнофункционално устройство. Не може да изпълнява ролята на PAN координатор или координатор. Може да оперира като крайно устройство, RFD-Tx или RFD-Rx устройство.

IEEE 802.15.4 топологии





IEEE 802.15.4 топология “Звезда”

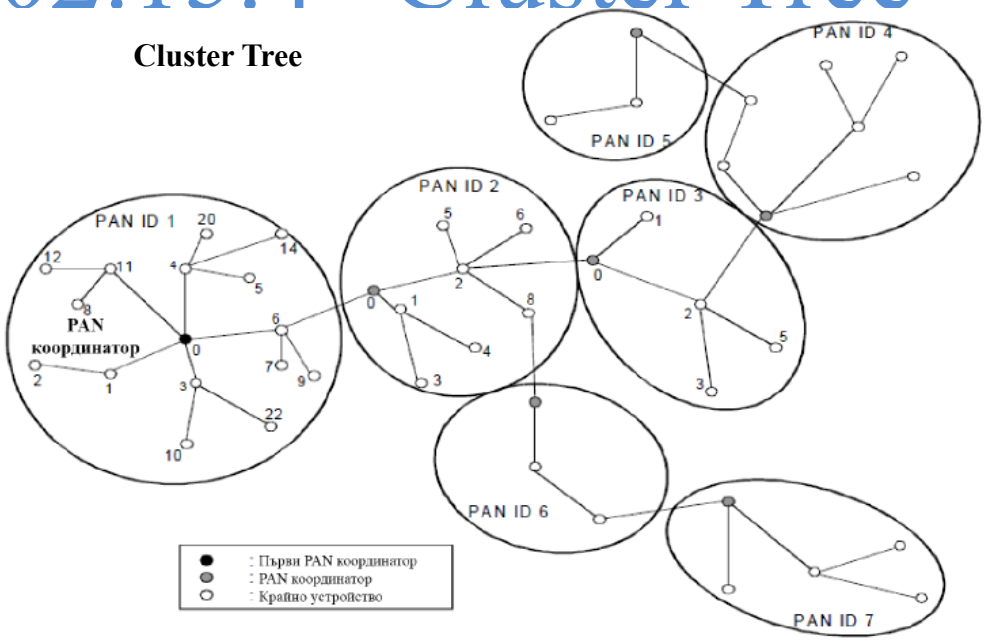


•Комуникацията между всички крайни устройства се осъществява през един централен контролер (PAN координатор).
•Крайните устройства (листата) могат да бъдат както пълнофункционални (FFDs), така и с намалена функционалност (RFDs).
•След като се активира едно пълнофункционално устройство, то може да установи негова собствена мрежа и да приеме ролята на PAN координатор на мрежата.
•Всяка PAN мрежа има собствено PAN ID, което е уникално, не е присвоено от друга PAN мрежа в радиообхвата на текущата и позволява независимо опериране на отделните мрежи, изградени с топология “Звезда”.
•След установяване на PAN ID, PAN координаторът позволява на останалите устройства (пълнофункционални и такива с намалена функционалност) да се свържат към неговата мрежа.
•Това е подходяща топология за изграждане на мрежи за домашна автоматизация, персонални компютърни периферни устройства, игри и лични здравни грижи.

IEEE 802.15.4 “Peer-to-peer” топология

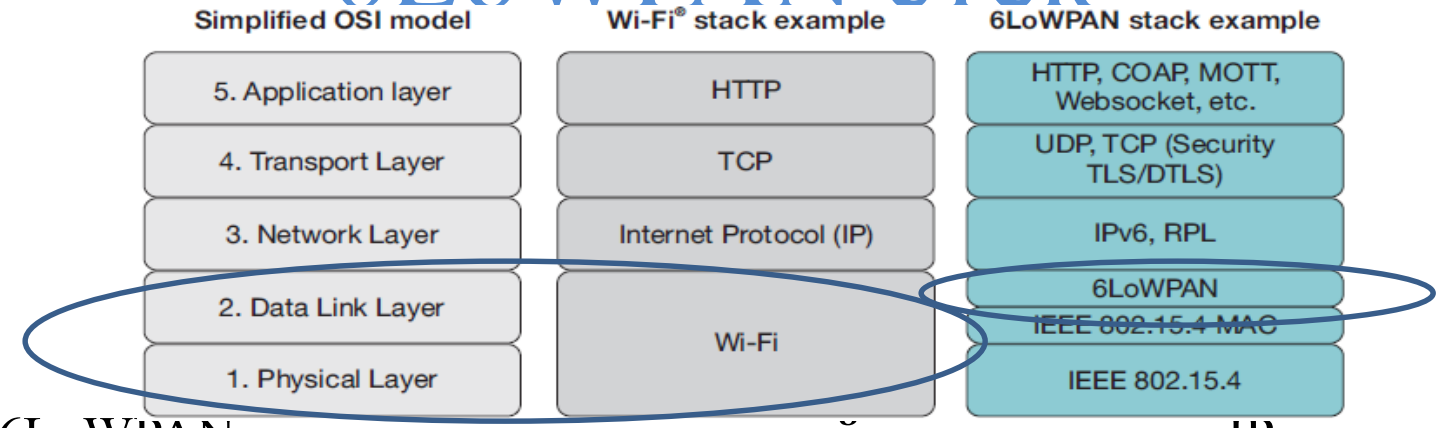
•има PAN координатор, но се различава от топология “Звезда” по това, че всяко устройство е в състояние да комуникира директно с всяко друго устройство в PAN мрежата, което се намира в радиообхвата му.
• Позволява рутиране на съобщение през множество хопове - от което и да е към което и да е устройство в конкретната мрежа.
•Намира приложение в мрежи за промишлен контрол и наблюдение, безжични сензорни мрежи, проследяване на активите и инвентара, интелигентно земеделие и сигурност.

IEEE 802.15.4 “Cluster Tree” топология



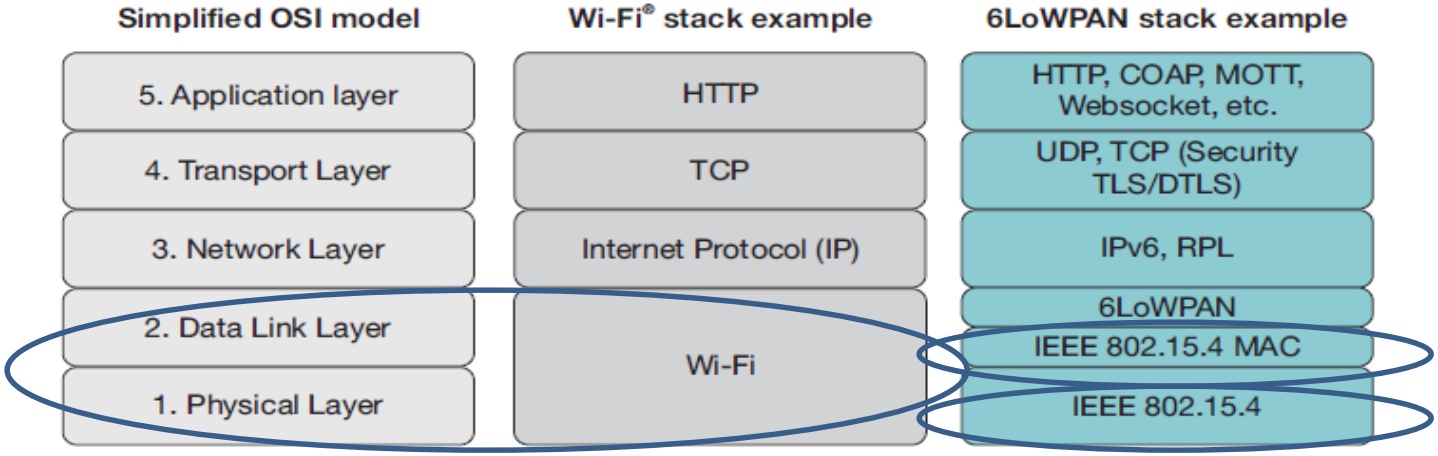
• специален случай на “Peer-to-peer” топологията.
•При тази топология повечето от устройствата са пълнофункционални, като тези с ограничена функционалност се свързват като листа (крайни устройства) към cluster tree мрежата на края на разклонението, тъй като те не позволяват на други устройства да се свързват към тях.
•Всяко пълнофункционално устройство е в състояние да бъде координатор и да осъществява синхронизиращи услуги за други устройства или координатори.
• Само един от всички тези координатори е основният PAN координатор, който обикновено има по-високи изчислителни ресурси от всяко друго устройство в PAN мрежата. PAN координаторът формира първия клъстер, като избира свободно PAN ID и изпраща сигнални (*beacon*) фреймове към съседите си. Устройството, което получава този фрейм, може да поиска да се присъедини към мрежата на PAN координатора. Ако той позволява това – добавя устройството като негово “дете” в списъка си със съседи. Нововключеното устройство добавя PAN координатора като “родител” в неговия списък със съседи и започва периодично да изпраща beacon сигнали. Към неговата мрежа могат да се свържат и други устройства.

6LoWPAN стек



- Чрез 6LoWPAN се въвежда адаптивен слой между стека за IP връзка и мрежовия слой, за да може да се предават IPv6 дейтаграми по IEEE 802.15.4 безжични връзки.
- Стандартът отговаря за:
  - активацията и деактивацията на радио приемо-предавателя,
  - откриване на енергия,
  - индикация за качеството на връзката,
  - оценка за чистотата на каналите и избор на канал,
  - разпространение, предаване и приемане на пакети през физическата среда.
- В допълнение към версията на стандарта от 2006г. съществуват две важни изменения:
  - IEEE 802.15.4e - цели по-нататъшно намаляване консумацията на електроенергия и подобряване на интерфейса.
  - IEEE 802.15.4g представлява изменение на PHY (физически) слой и има за цел да осигури допълнителна гама радиочестотни ленти.

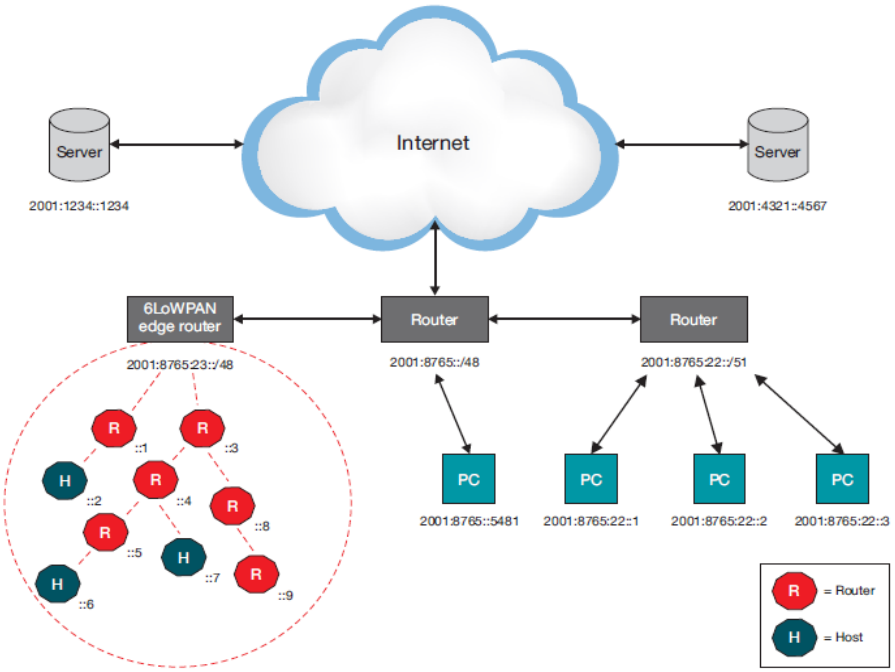
6LoWPAN стек



•Data-Link слоят осигурява надеждна връзка между два директно свързани възела, чрез откриване и коригиране на грешки, които могат да възникнат във физическия слой по време на предаване и получаване.
•Data-Link слой включва в себе си MAC, който осигурява достъп до комуникационната среда, използвайки функции като Carrier Sense Multiple Access – Collision Avoidance (CSMA-CA), при която средата се прослушва за това дали някой предава преди да се извърши изпращането на данни.
•Data-Link слой обработва и данновите фреймове.

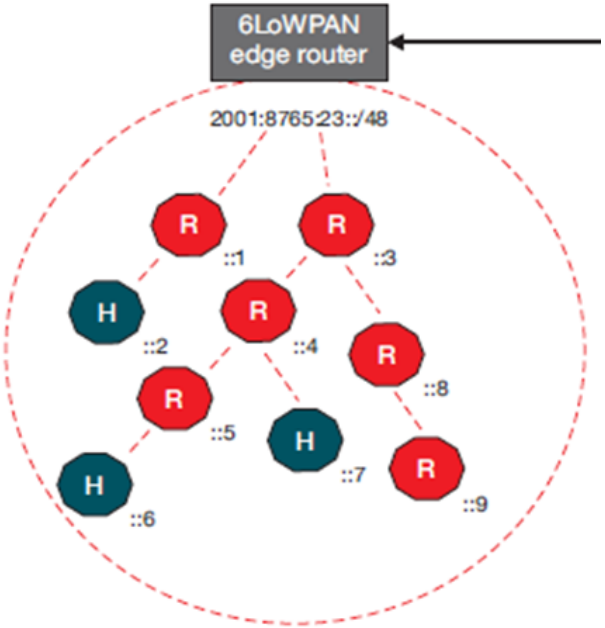
•При 6LoWPAN, MAC слоят е IEEE 802.15.4.
•Адаптивното ниво 6LoWPAN, което осигурява адаптиране от IPv6 към IEEE 802.15.4, също се намира в Data-Link слоя.

6LoWPAN



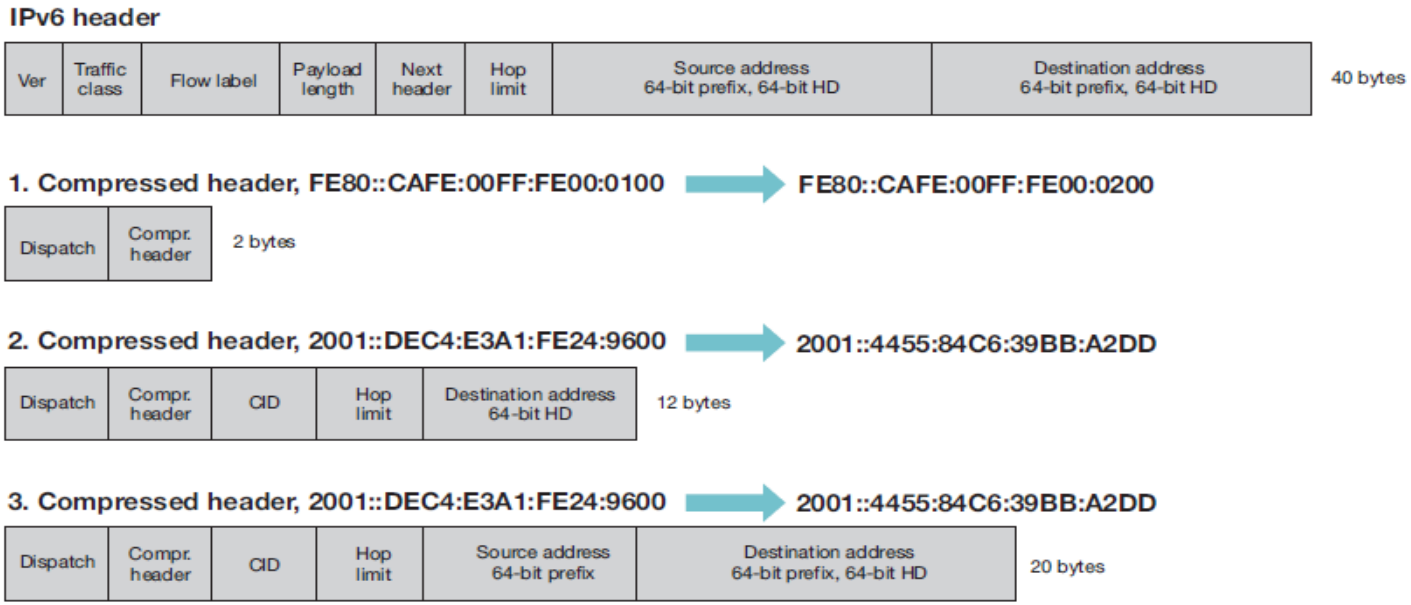
- Чрез комуникация основно по IP, 6LoWPAN мрежите са свързани с други мрежи, като се използват IP маршрутизатори.
- 6LoWPAN мрежите обикновено работят в периферията, действайки като Stub мрежи. Това означава, че постъпващите данни са предназначени за едно от устройствата в 6LoWPAN мрежата.
- Една 6LoWPAN мрежа може да бъде свързана към други IP мрежи чрез един или повече Edge маршрутизатори, които препращат IP дейтаграми между различни преносни среди. Свързването с други IP мрежи може да се осигури чрез произволна връзка, като например Ethernet, Wi-Fi или 3G/4G/5G.

6LoWPAN



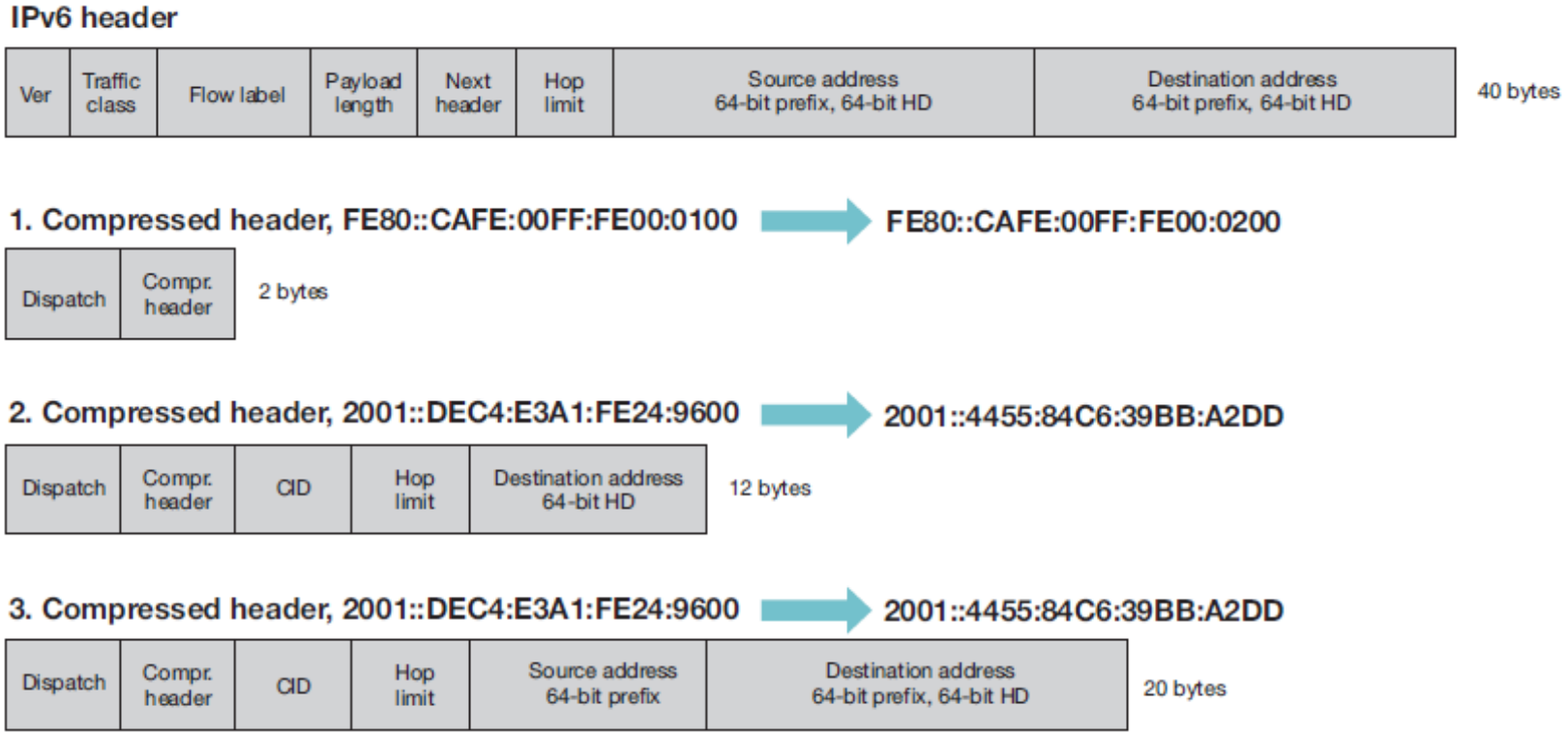
- При 6LoWPAN мрежи, връзката с Интернет се обработва от Access Point (AP), действащ като IPv6 рутер.
- Към AP може да бъдат свързани няколко различни устройства като PC, сървър и т. н.
- 6LoWPAN мрежата се свързва с IPv6 мрежа с помощта на Edge Router.
- Edge маршрутизаторът извършва три действия:
  - обмен на данни между 6LoWPAN устройства и Интернет (или друга IPv6 мрежа);
  - обмен на данни между устройства в 6LoWPAN мрежата;
  - генериране и поддръжка на подмрежа със 6LoWPAN радиосвързаност.

Компресия на хедърите при 6LoWPAN - причини



- Устройствата, които имплементират 6LoWPAN, обикновено са ограничени по отношение на ресурсите си – имат около 16 kB RAM и 128 kB ROM.
- За да се позволи пренасянето на IPv6 (40 bytes), TCP (20 bytes) и UDP (8 bytes) хедъри през 802.15.4 радиовръзка, адаптивният слой осигурява компресиране на хедърната информация, както и фрагментиране и реасемблиране на данните.

Компресия на хедърите при 6LoWPAN - реализация

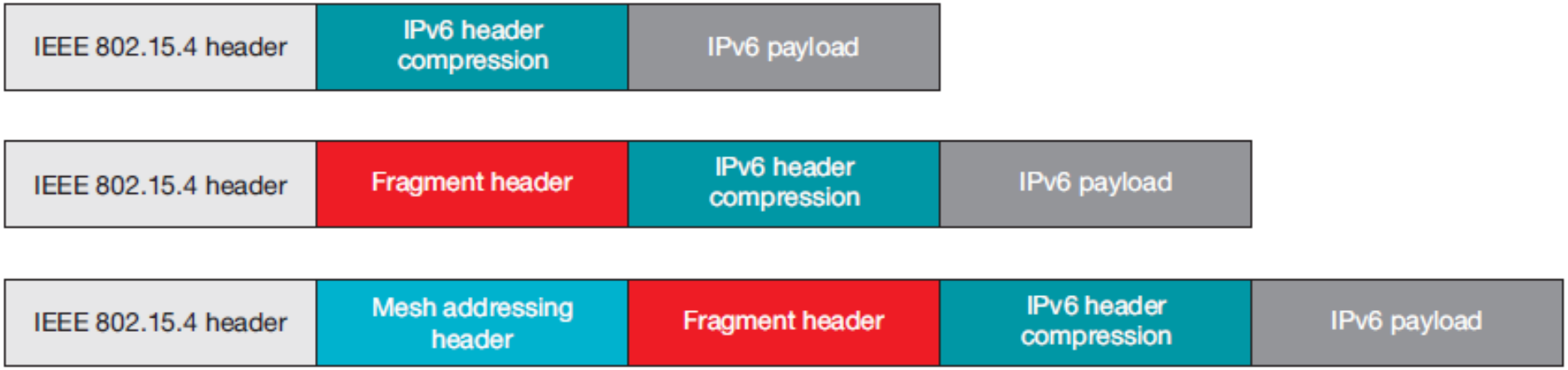


1. Комуникация между две устройства в една и съща 6LoWPAN мрежа – чрез използване на локални адреси, IPv6 хедъра може да бъде компресиран до 2 байта;
2. Ако комуникацията е насочена към устройство извън 6LoWPAN мрежата и префикса на външната мрежа е известен, IPv6 хедъра може да бъде компресиран до 12 байта;
3. В случай че комуникацията е насочена към външно устройство, но префиксът не е известен, IPv6 хедъра може да бъде компресиран до 20 байта.

Фрагментиране и реасемблиране на IPv6 пакети

- IPv6 пакетите трябва да бъдат разделени на няколко по-малки сегмента, за да се позволи изпращането на IPv6 пакети (максимум 1280 байта) през IEEE 802.15.4 радиовръзки (127 байта MTU).
- За целта се добавя допълнителна информация в хедърите, която се използва за реасемблиране на пакетите в правилен ред.
- След получаване и реасемблиране на данновите пакети, допълнителната информация се премахва и пакетите се възстановяват до първоначалния им IPv6 формат.
- В зависимост от използваната технология за маршрутизиране са възможни два случая:
  - при *mesh-under* рутиране – фрагментите се реасемблират само при получаване от крайната дестинация;
  - при *route-over* рутиране – фрагментите се реасемблират на всеки хоп.
- В случай че трансфера на фрагменти е неуспешен, целият IP пакет трябва да бъде изпратен отново.

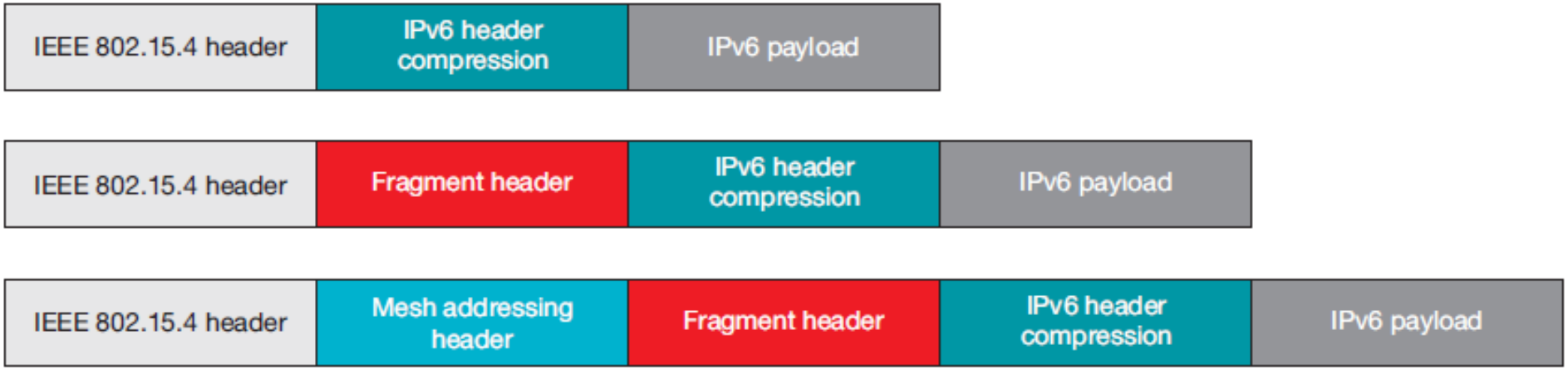
6LoWPAN хедъри



6LoWPAN дефинира три типа хедъри, които определят възможностите на фрейма:

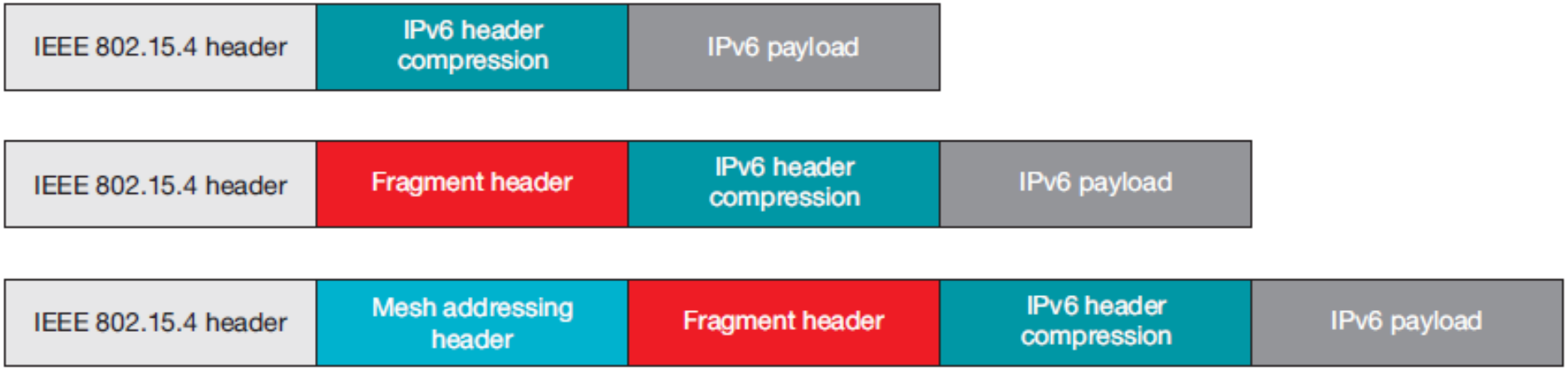
- mesh
- фрагментиращ
- компресиран

6LoWPAN хедъри-mesh



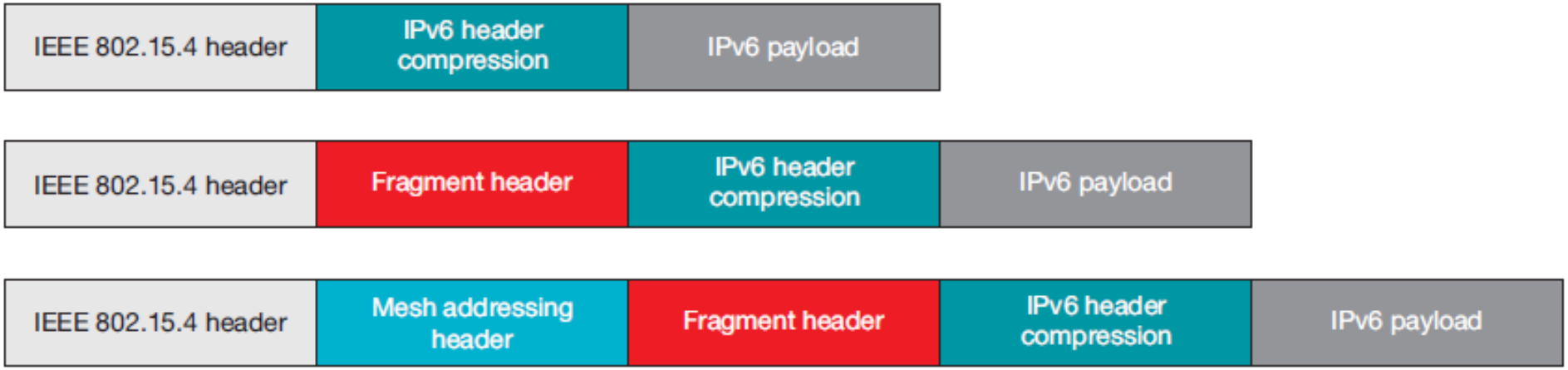
- Поддържа препращане на Data-Link слоя;
- Не се използва при изпращане на данни само през един хоп;
- Съдържа три полета:
  - лимит за хоповете – използва се за ограничаване броя на хоповете при препращане; при всеки хоп се намаля с 1; ако броячът достигне 0, то пакетът се изхвърля;
  - адрес на източника;
  - адрес на дестинацията;

6LoWPAN хедъри- фрагментиращ



- Поддържа предаването на IPv6 MTU;
- Използва се, когато информацията е твърде голяма, за да се побере в един IEEE 802.15.4 фрейм;
- Има три полета:
  - размер на дейтаграма - описва реасемблираната дейтаграма;
  - етикет на дейтаграма – идентифицира групата фрагменти;
  - изместване – описва изместването на фрагмента в реасемблирания полезен товар.

6LoWPAN хедъри- компресиран



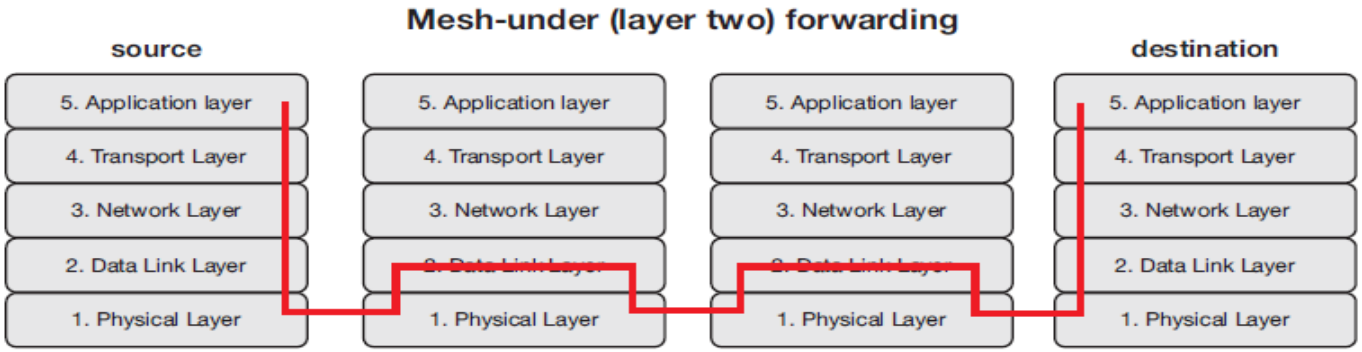
- Използва се при препращане на пакети от множество хопове в рамките на 6LoWPAN мрежа.
- Има три полета:
  - Hop limit – използва се за указване на максималния брой хопове, които може да премине пакета. Стойността в полето намалява с единица при преминаване от всеки хоп. Когато брояча стигне до 0, пакета се отхвърля;
  - Source address;
  - Destination address.

Маршрутизиране при 6LoWPAN

В зависимост от това в кой слой се реализира маршрутизиращият механизъм, са дефинирани две категории маршрутизиране:

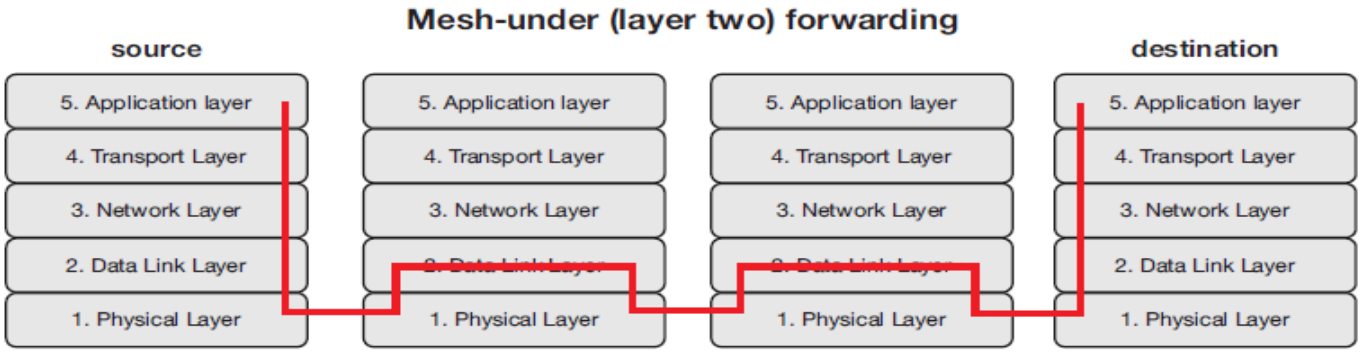
- Mesh-Under - за малки и локални мрежи.
- Route-Over – за по-мощни и големи мрежи.

Mesh-under маршрутизиране (1)



- Mesh-under (Direct Mode) използва адресиране на Data-Link нивото (IEEE 802.15.4 MAC или кратки адреси) за маршрутизиране на пакети.
- Маршрутизирането на данни при mesh-under системи се случва невидимо, следователно mesh-under мрежите трябва да бъдат в един IP събнет.
- Единственият IP рутер в тези системи е *edge* маршрутизаторът.
- За да се осигури съвместимост с IPv6 протоколи от по-високи слоеве, като "*откриване на дублирани адреси*" (DAD), се установява само един броудкаст домейн. Тъй като тези съобщения трябва да бъдат изпращани до всички устройства се получава натоварване на мрежата.

Mesh-under маршрутизиране (2)



•Mesh-under схемата препраща пакети през множество радиохопове, като не ги третира като IP хопове, мрежовият слой не участва в рутирането.

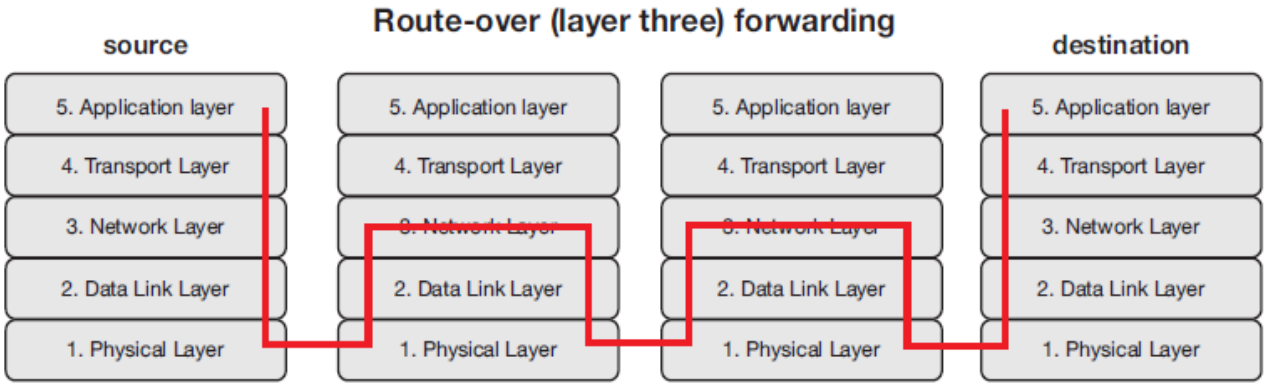
•Адаптивният слой разглежда всеки входящ фрагмент еднакво. Когато фрагмент трябва да бъде пренасочен, се добавя mesh хедър в началото на 6LoWPAN хедъра, след което информацията, съдържаща се в mesh хедъра, е комбинирана с адреса на източника и адреса на получателя.

•При получаване на пакет с mesh хедър, възелът проверява адреса на получателя, за да провери дали пакетът е за него.

–В случай че не е, пакетът се препраща, а информацията в mesh хедъра се обновява с адреса на следващия хоп и стойността на полето “оставащи хопове” се намаля с 1. Фрагментите се реасемблират само след като достигнат дестинацията.

– В случай на липсващ фрагмент източникът препраща отново всички фрагменти.

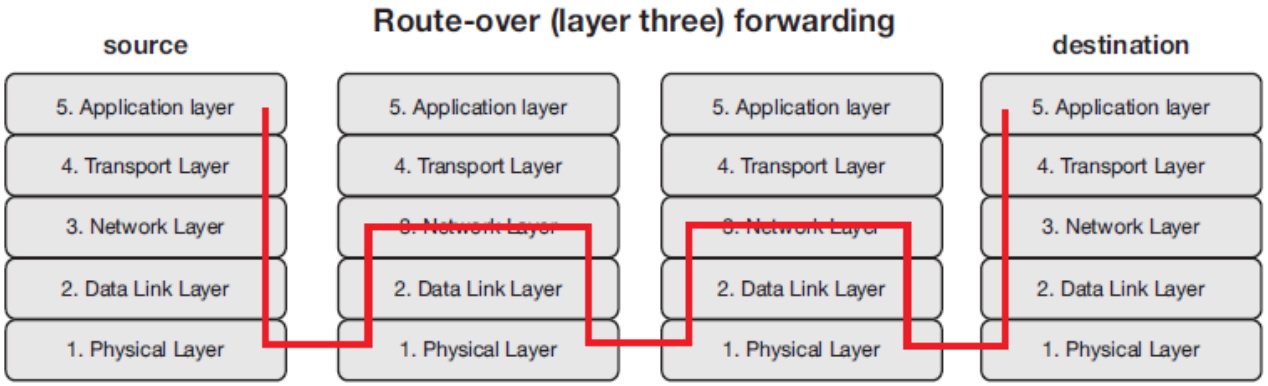
Route-Over маршрутизиране (1)



Route-Over използва адресиране на мрежово ниво (IP адреси).

- Всеки хоп изпълнява ролята на IP рутер.
- Най-широко използваният протокол за маршрутизация при route-over системи е RPL (Routing Protocol for Low-Power and Lossy Networks).
- Той поддържа два маршрутизиращи режима:
  - Storing режим – всички устройства в 6LoWPAN мрежата, които са конфигурирани като маршрутизатори, поддържат рутинг таблица и таблица на съседите си;
  - Non-storing режим – единственото устройство, което поддържа своята рутинг таблица, е Edge маршрутизатора. Използва се Source рутинг, което означава, че изпращаният пакет съдържа в себе си целия път, който трябва да измине, за да достигне до получателя.

Route-Over маршрутизиране (2)



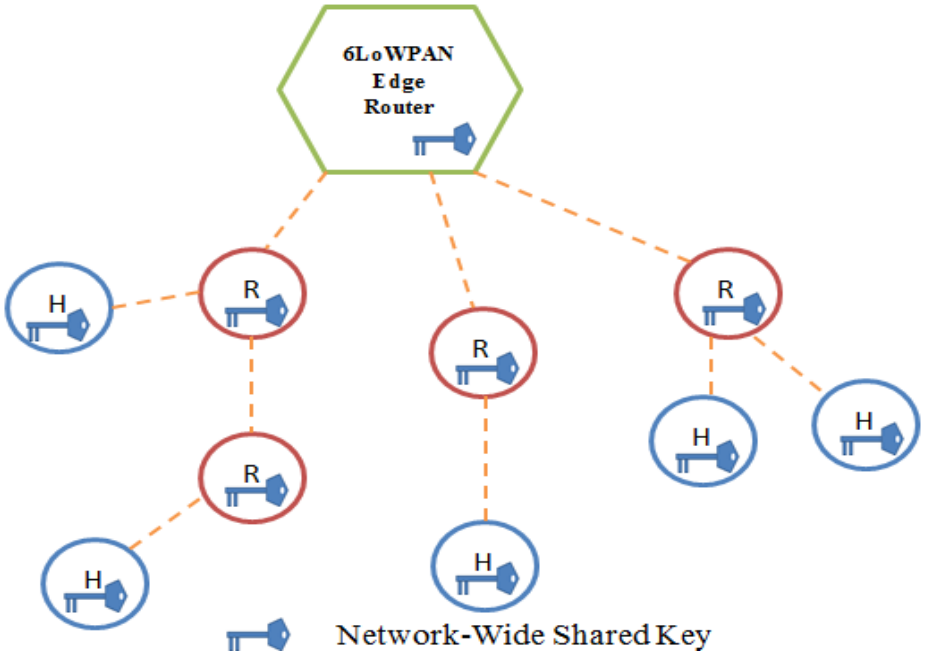
- В случай на фрагментация на пакет е необходимо получаването на всички фрагменти от адаптивния слой на всяко устройство.
- Той реасемблира целия пакет, за да провери дали е получателят му.
- В случай че пакетът трябва да бъде препратен, се фрагментира отново и се изпраща към следващ хоп, спрямо рутинг таблицата на устройството.
- При фрагментацията на пакета от адаптивния слой, той добавя хедър с информация дали това е първият фрагмент и номер на поредицата за следващите фрагменти.

Сигурност при 6LoWPAN

За реализиране на сигурността при 6LoWPAN се използват няколко метода:

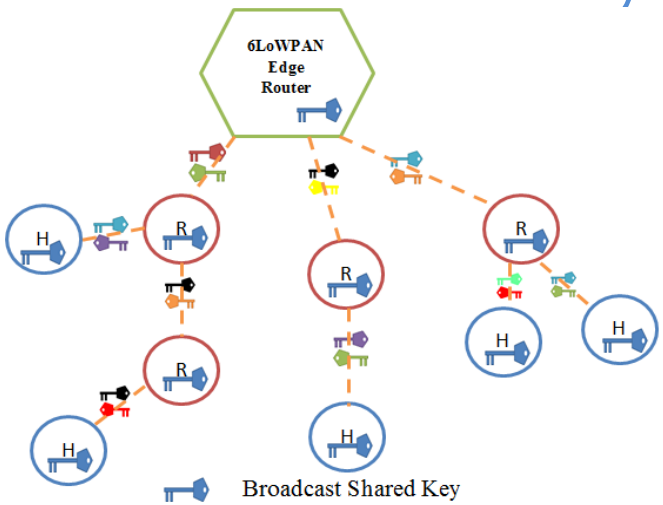
- Network-Wide Shared Key;
- Fully Pairwise Keys;
- Group Keying;
- Hybrid method.

Network-Wide Shared Key



•Всеки възел разполага с един и същ ключ за автентиткация в мрежата.
•Предварителното зареждане на всеки възел със споделен ключ в мрежата обаче не е добро решение, защото 6LoWPAN мрежите работят без надзор във враждебна среда, което прави тези мрежи податливи на компрометиране.
•При компрометиране на възела, атакуващият физически достъпва възела и отстранява крипто-ключа. След като нападателят получи споделените ключове в мрежата, може да изпрати произволни фреймове навсякъде по всяко време. Освен това, атакуващият може да добави неоторизирани възли към мрежата „жертва“.

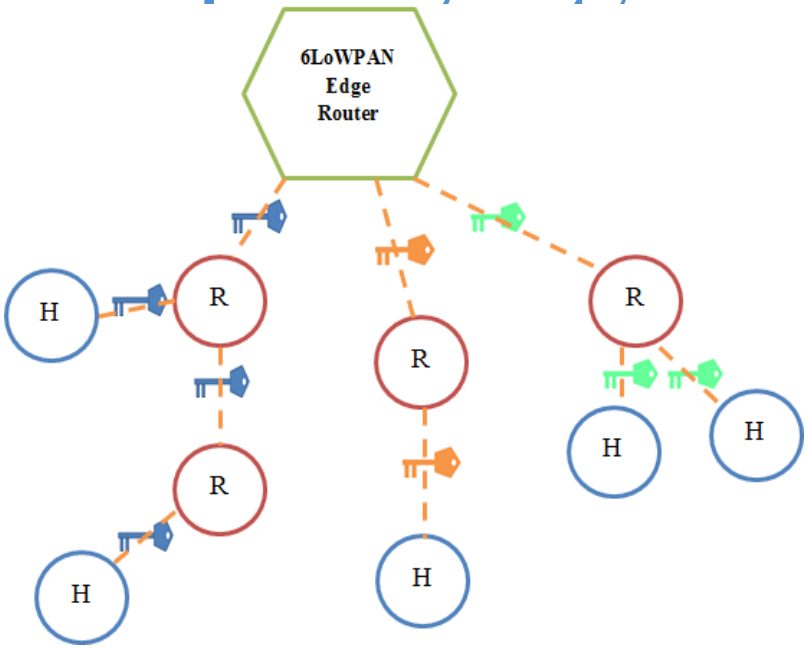
Fully Pairwise Keys



Всеки възел е предварително зареден с двойка ключове за комуникация с друг възел. При този метод компрометирането на възел засяга само стари и бъдещи съобщения, изпратени до или от този възел. Останалия трафик, предаван между другите възли е незасегнат. Това е по-устойчив метод срещу компрометиране, но има три основни проблема:

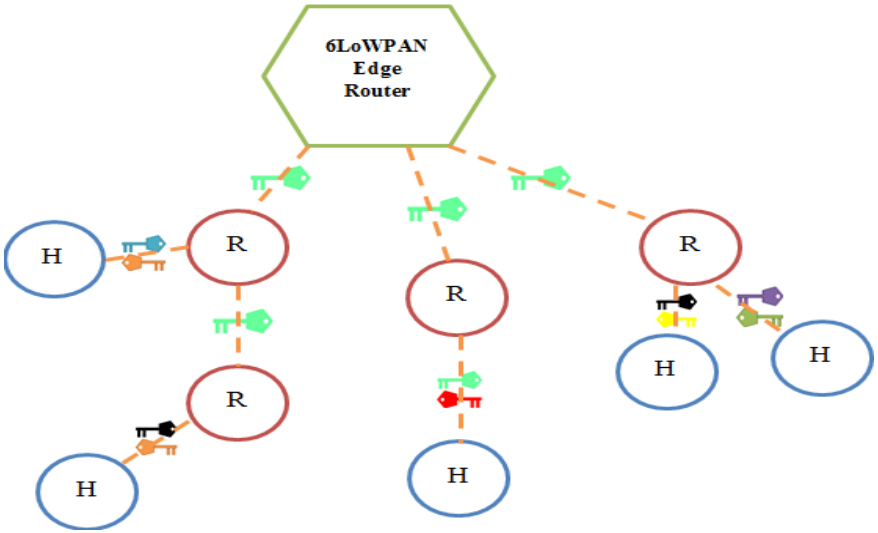
- за широкомащабни 6LoWPAN мрежи тази схема може да заеме твърде много памет при съхраняване на двойките ключове, тъй като за всеки съсед се използва различна двойка ключове;
- възникват проблеми с управлението на броячите на фреймове. За да се открият преименувани фреймове е необходимо да се съхрани най-новият брояч на фреймове за адреса на източника, което заема памет и може да е необходимо да се използва флаш памет, която изисква голямо количество енергия;
- докато двойките ключове предлагат решение, което е устойчиво на компрометиране на Unicast фреймовете, не се предоставя подобно решение за Broadcast фреймовете. Broadcast фреймовете трябва да се автентицират с ключове, които са споделени между съседните възли.

Group Keying



- Компромисен вариант между Network-Wide Shared Key и Fully Pairwise Keys методите.
- При този метод един ключ се споделя между множество възли и се използва за автентициране между всеки два възела в тази група. Разделянето по групи може да се извършва въз основа на местоположение, мрежова топология или сходство на функцията.
- Предимството на „Group Keying“ метода е, че осигурява междинен вариант между Network-Wide Shared Key и Fully Pairwise Keys методите с частична устойчивост срещу компрометиране на възлите за по-ниска цена.

Hybrid method



- Някои системи може едновременно да ползват разгледаните механизми за автентикация в едно и също приложение.
- Например може да се използва Full Pairwise Keys механизъм за автентициране за всички връзки между възел и базова станция и да се използва Network-Wide Shared Key метод за всички останали връзки в мрежата.

Мобилност при WSN и MSN

- IPv6-based протоколи

IPv6-based mobility protocols				
Macro mobility			Micro mobility	
MIPv6	FMIPv6	NEMO	PMIPv6	
MIPv6 and MOBINET	Inter MARIO	SNEMO	SPMIPv6	CSPMIPv6

- Host-based и Network-based протоколи за извършване на мобилност

Host-based (Node-based) mobility scheme	Network-based mobility scheme
MIPv6 and MOBINET **HMIPV6** **Inter MARIO**	SNEMO SPNIPV6 CSPMIPV6 PMIPV6 Inter MARIO

Качество на услугите при 6loWPAN

Реализира се на:

- Приложно ниво
- Мрежово ниво
- Ниво на възприемане на данните

Алгоритми за планиране на трафика:

- Knowledge Free алгоритми - обработват заявките в реда на тяхното получаване;
- Knowledge Based алгоритми - използват информация за приложенията, за мрежата или и двете, за да приоритизират трафика

Въпроси ?

Благодаря за вниманието !

Литература:

- https://www.slideshare.net/linaroorg/linuxwpan-ieee-802154-and-6lowpan-in-the-linux-kernel-bud17120
- https://www.techbriefs.com/component/content/article/tb/supplements/st/features/articles/27510