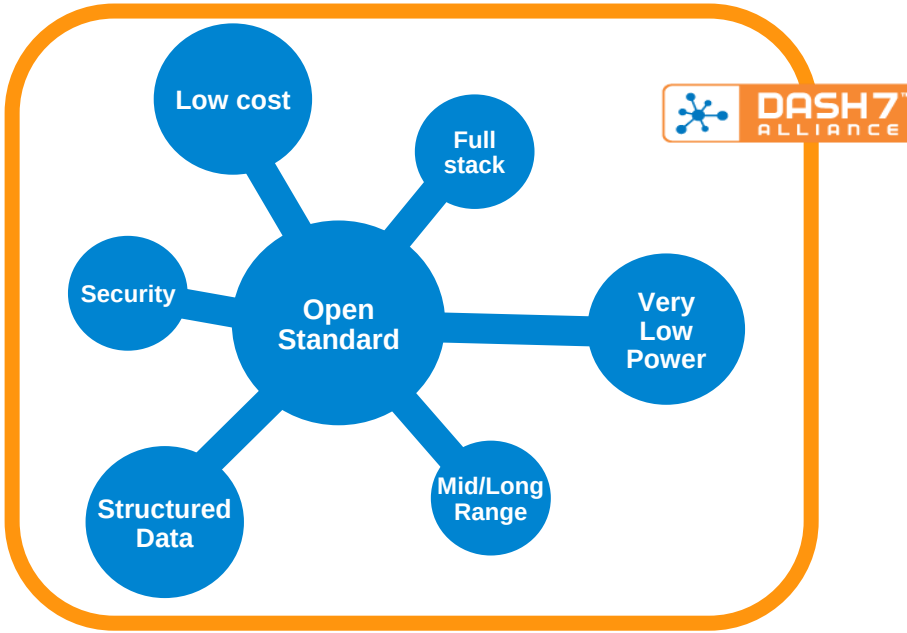
DASH7 ALLIANCE PROTOCOL - WHERE RFID MEETS WSN

DASH7 ALLIANCE PROTOCOL

OPEN STANDARD OF ULTRA LOW POWER MID-RANGE SENSOR AND ACTUATOR COMMUNICATION

- Wireless Sensor and Actuator Network Protocol (WSAN)
- Originates from ISO 18000-7 (“dash7”)
  - describes the parameters for active air interface communications at 433 MHz (2008 - 2009)
- Extended to support IoT functionalities
- Now support all sub-GHz ISM/SRD bands
- Star or tree network topology (no mesh)
- v1.1 of the spec published in Q1 2017.
- Active members of the Protocol Action Group:
  Wizzilab, University of Antwerp, Wroclaw Technical University and CORTUS



BLAST networking technology

Bursty
Data transfer is abrupt and does not include content such as video, audio, or other isochronous forms of data

Light
For most applications, packet sizes are limited to 256 bytes. Transmission of multiple, consecutive packets may occur but is generally avoided if possible.

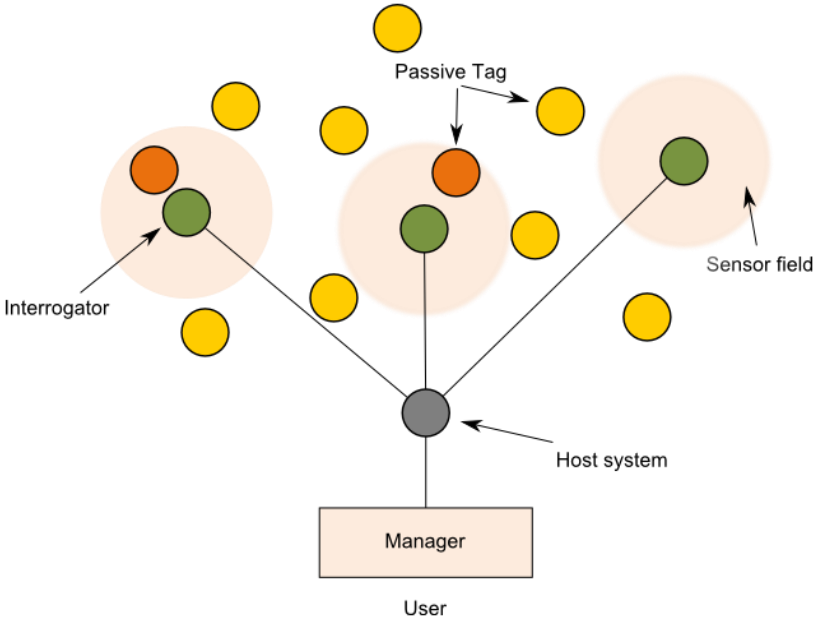
Asynchronous
DASH7's main method of communication is by command-response, which by design requires no periodic network "hand-shaking" or synchronization between devices.

Stealth
DASH7 does not use discovery beacons, end nodes can chose to respond only to pre-approved devices.

Transitional
A DASH7 system of devices is inherently mobile or transitional. Unlike other wireless technologies DASH7 is upload-centric, not download-centric, thus devices do not need to be managed extensively by fixed infrastructure (i.e. base stations) to respond only to pre-approved devices.

NETWORK TOPOLOGY

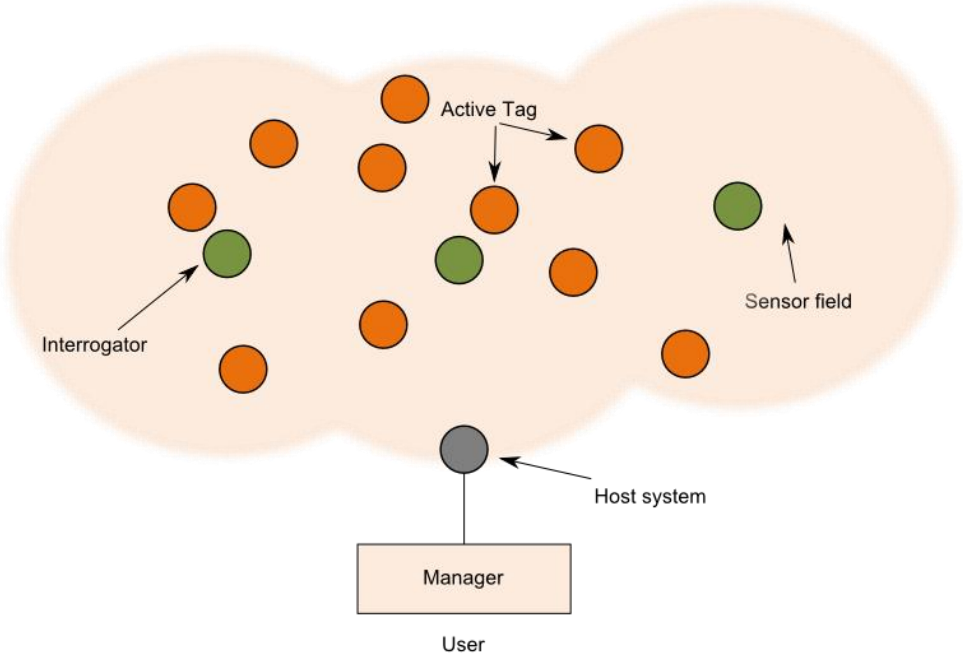
PASSIVE RFID



- Tags can only be read in the immediate proximity of a reader

NETWORK TOPOLOGY

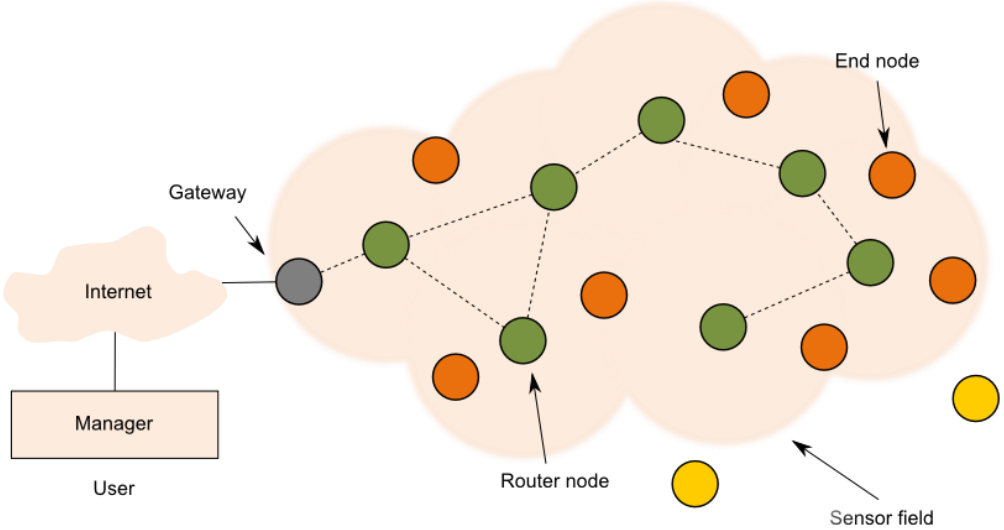
ACTIVE RFID



- Longer range interrogators - Master/Slave

NETWORK TOPOLOGY

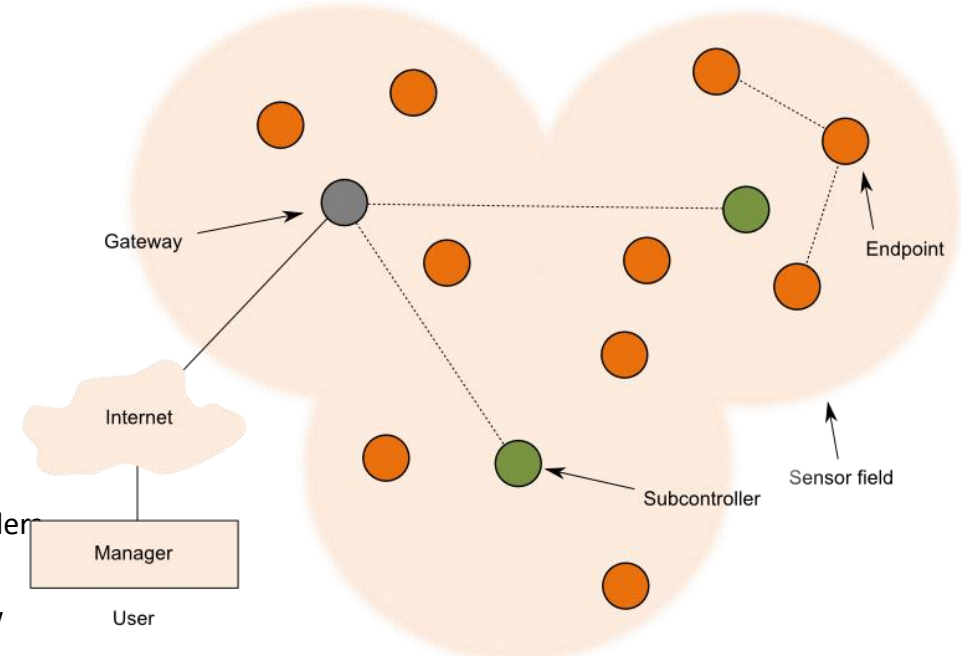
MESH WSN



- Range depends on number of router nodes
- Congestion - Routing complexity
- Latency due to propagation through the network
- Routers need to be powered and add to the overall consumption of the system

NETWORK TOPOLOGY

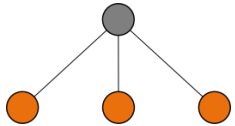
DASH7



- Range of Gateway can be extended by subcontroller
- Simple routing (2 hops)
- Subcontrollers need to be powered but only a few are needed
- Tag-2-Tag communication

NETWORK TOPOLOGY

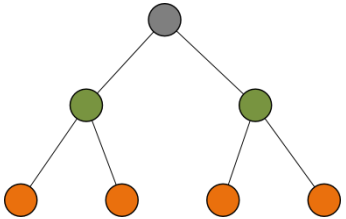
Star



Passive RFID
Tags can only be read in the intermediate proximity of a reader

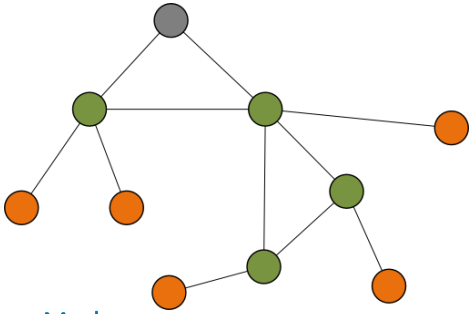
Active RFID
Longer range interrogators – Master/Slave

Tree



DASH7
Simple routing (2 hops)
subcontrollers are power but only few are needed
Tag-to-Tag & Tag-Talk-First

Mesh

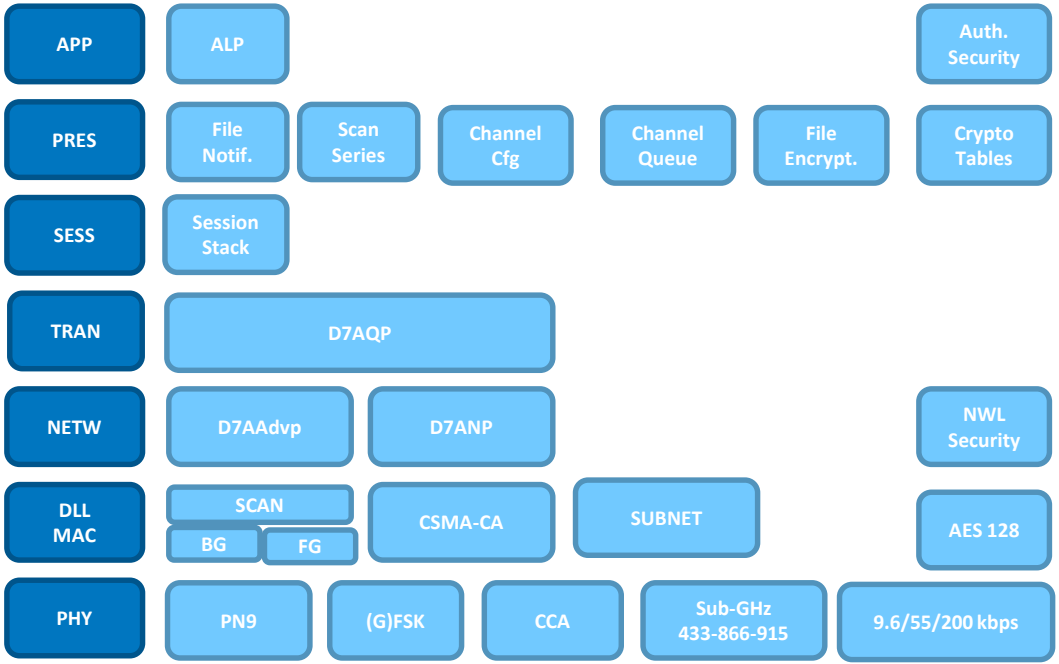


Mesh
Range depends on number of router nodes

Congestion – Routing Complexity – Latency
Routers need to be powered
Each hop consumes energy

Distance – Complexity – Energy – Latency

FULL STACK SPECIFICATION



OSI Layer		D7AComponent	Description
7	**Application**	File Access	File management via Application Layer Programming Interface (ALP). Property-based queries.
		D7AActP	Pre-registered application actions, triggered conditionally on file access.
6	**Data Elements**	D7A Files	A user-driven file system that supports read, write, create, delete, modify of executable, encryptable files.
			Native attributes allowing to configure D7AActP actions triggered on file access.
5	**Session**	D7ASP	Session FIFOs, priorities and QoS management.
4	**Transport**	D7ATP	Request-Response and group acknowledgment.
3	**Network**	D7ANP	Routing (no-hop & one-hop), foreground scan automation
		D7AAdvP	Ad-hoc synchronization
		Addressing	Access Profile
		Security	AES-128 authentication and encryption
2	**Data Link**	Frame Addressing Data	Unicast, Broadcast
		Transmission	Upper-layer event driven
		Data Reception	Upper-layer event driven, or via configurable, sequential automated channel scan
		Channel Access	CSMA-CA, with static channel guarding rules, multiple supported flow/congestion control models and frequency diversity.
1	**Physical**	Channel QoS	Clear Channel Assessment
		Encoding	1/1 PN9, 1/2 convolutional Code
		Rates	9.6 kb/s, 55.55 kb/s, 166.667 kb/s
		Modulation	± 4.8 kHz 2-(G)FSK, ± 50 kHz 2-(G)FSK or ± 41.667 kHz 2-(G)FSK
		Channel spacing	25 kHz or 200 kHz
		Spectrum	433.060 – 434.785 MHz 863.000 – 870.000 MHz 902.000 – 928.000 MHz

APPLICATION LAYER PROTOCOL

EVERYTHING IS A FILE

Structured data

- Everything is a file (sensor values, system configuration, encryption keys...)
- Any application action, data exchange method or protocol is mapped exclusively onto manipulation of Structured Data Elements (D7A Files) and their properties.

ALP

- ALP is a generic API for manipulating D7A files. The interface can be D7A, but also UART, BTLE
- **ALP commands** are composed of **ALP Actions**
- Actions can be read, write, create, delete, execute, condition (query), grant permission, etc...
- Local or OTA

QUERIES + ACTIONS + D7A

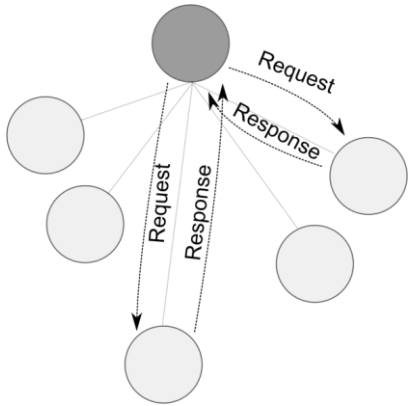
=

DISTRIBUTED DATABASE

Communication Model

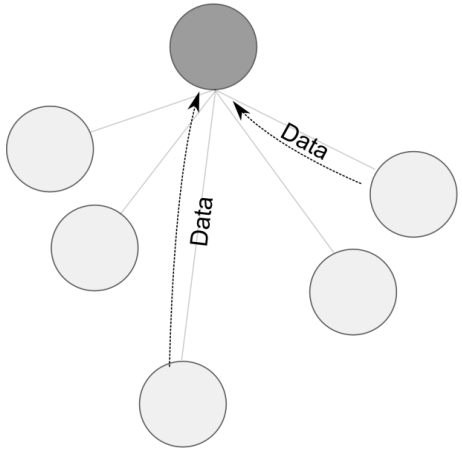
Pull

To obtain tag sensor data
To set actuator data



Unsollicited – Tag Talk First

For alarms and periodic data

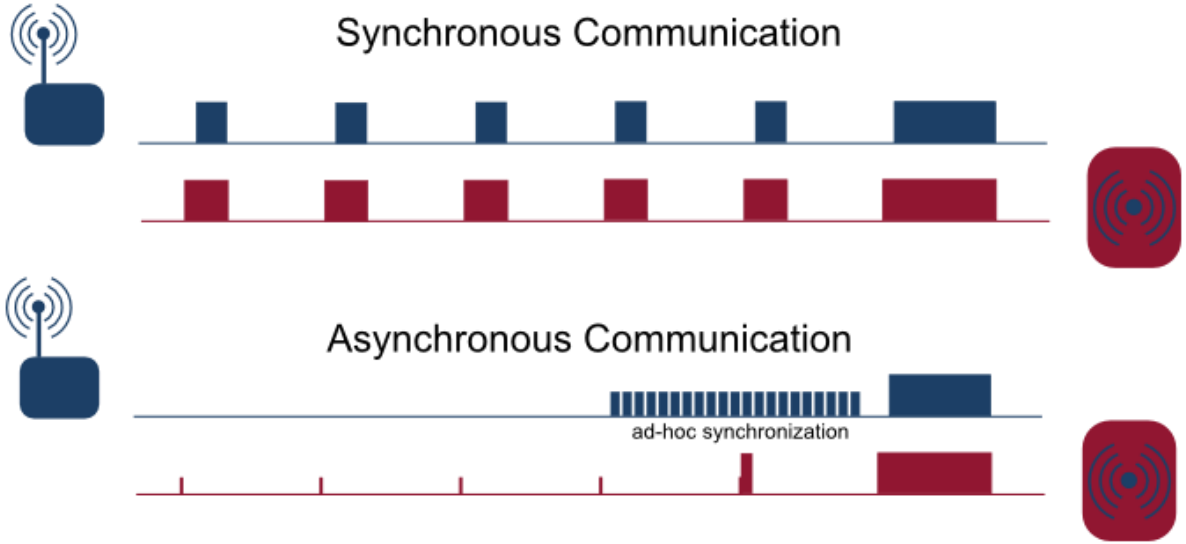


- Polling data using D7AP Advertising Protocol
- Pushing data using D7AP Action Protocol
- Dormant sessions (wait for the tag to talk first)

COMMUNICATION SCHEMES

D7AADVP

- Advertisement protocol
- Gateway queries endpoints
- Low power wake—up



COMMUNICATION SCHEMES

D7AACTP

- Action protocol
- Notification / tag-talks-first
- ALP command preregistered on endnodes
- Filesystem can be configured to activate ALP command upon file access

COMMUNICATION SCHEMES

D7AACTP – APPLICATION EXAMPLE

Humidity Notification

Send a message to 0x23BE with the humidity and the battery level when the humidity changes.

Battery Alarm

Broadcast battery alarm when battery below 20% and send all latest sensor values.

Sensor on Presence

When the presence is detection from a mobile device and temperature is below 21°C, send ‘on’ command to local heating.

COMMUNICATION SCHEMES

D7AACTP - IMPLEMENTATION IN APPLICATION FIRMWARE

Humidity Notification

Measure humidity at x sec interval and write value to file with ID 0x34

Battery Alarm

Measure battery at x sec interval and write value to file with ID 0x25

Sensor on Presence

Measure temperature at x sec interval and write value to file with ID 0x33

COMMUNICATION SCHEMES

D7AACTP - CONFIGURATION OF FILE SYSTEM

Humidity Notification

Configure notification header for file 0x34 and set query to condition different from previous value. Set 0X23BE and 0x34 in notification file.

Battery Alarm

Configure notification header for file 0x25 and set query to condition
< 20. Set 0x25, 0x34 and 0x33 in notification file.

Sensor on Presence

Configure notification on file 0x19 (localisation file) and set 0x33 in in the notification file.

COMMUNICATION SCHEMES

TRADE-OFFS

D7AAdvP

Ideal for ad-hoc data gathering, not for periodic or sensor triggered.

Tradeoff between energy consumption and latency

D7AActP

Ideal for periodic sensor data transmission or sensor triggered

- Dormant sessions
- Use case specific, combinations possible
- Network behavior over-the-air updatable

CONTEXT AWARE SENSOR AND ACTUATOR DATA PROPAGATION

Write and read from files

Configure system through configuration files

DASH7 ALLIANCE

Configured through file system

Handles scheduled scan cycles

Handles queries from other devices

Handles queries and notifications on file changes

File system configurable over the air

D7 DATA ELEMENTS

Content	Length (bytes)	Offset (bytes)	Type	Description
Permissions	1	0	u8	As defined in 10.1.4.1
Properties	1	1	u8	As defined in 10.1.5.1.
ALP Command File ID	1	2	u8	Index of the File containing the ALP Command, executed by D7AActP. Discarded if the ACT_EN field in Properties is set to 0.
Interface File ID	1	3	u8	Index of the File containing the Interface, on which the result of D7AActP is sent. Discarded if the ACT_EN field in Properties is set to 0.
File Size	4	4	u32	Current size of the file.
Allocated Size	4	8	u32	Size, allocated for the file in memory (appending data to the file cannot exceed this value)

Table 10.1.6.1: File Header

Definition	Code	Description
Transient	0	The content is not kept in memory. It cannot be read back.
Volatile	1	The content is kept in a volatile memory of the device. It is accessible for read, and is lost on power off.
Restorable	2	The content is kept in a volatile memory of the device. It is accessible for read, and can be backed-up upon request in a permanent storage location. It is restored form the permanent location on device power on.
Permanent	3	The content is kept in a permanent memory of the device. It is accessible for read and write.

Table 10.1.2.1: Storage Classes

b7	**ACT_EN**	When set, D7AActP is enabled
b6-b4	**ACT_COND**	Type of access that triggers D7AActP. Discarded if ACT_EN is set to 0. 0 – list (check for existence), 1 – read, 2 – write, 3 – write-flush, 4-7 – RFU
b3-b2	**RFU**	
b1-b0	**STORAGE CLASS**	As defined in 10.1.2

Table 10.1.5.1: File Properties

D7 DATA ELEMENTS

FILE ID LIST

ID	Description	Reference
0x00	UID	10.3.1
0x01	Factory Settings	10.3.2
0x02	Firmware Version	10.3.3
0x03	Device Capacity	10.3.4
0x04	Device Status	10.3.5
0x05	Engineering Mode	10.3.6
0x06-0x07	RFU	
0x08	PHY Configuration	10.3.7
0x09	PHY Status	10.3.8
0x0A	DLL Configuration	10.3.9
0x0B	DLL Status	10.3.10
0x0C	NWL Routing	10.3.11
0x0D	NWL Security	10.3.12
0x0E	NWL Security Key	10.3.13
0x0F	NWL Security State Register	10.3.14
0x10	RFU	
0x11	TRL Status	10.3.15
0x12	SEL Configuration	10.3.16
0x13	SEL Status	10.3.17
0x14-17	RFU	
0x18	Root Authentication Key	10.3.18
0x19	User Authentication Key	10.3.19
0x1A	Location Data	10.3.20
0x1B	ISO 21451-7 Sensor Description	10.3.21
0x1C	RTC	10.3.22
0x1D-0x1F	RFU	
0x20+I	Access Profile of Access Specifier I ∈ [0, 14]	10.3.23

SESSION LAYER

- Defines the method for queuing, scheduling, transmitting, retransmitting and receiving upper layer Requests
- Defines the QoS
- Destination Access parameters
- Power Autoscaling

State	Code	Description
Idle	0	Inactive / Terminated Session
Dormant	1	The group of Requests needs to be executed within a timeout period, which has not expired. After completion of the period, the Dormant Session is transformed into Pending Session.
Pending	2	The group of Requests needs to be executed as soon as possible.
Active	3	The Session is being currently executed using the D7A Session Protocol.

Table 9.1.3.1: Master Session States

State	Code	Description
Idle	0	Terminated Session
Active	3	Session is being currently executed

Table 9.1.2.1: Slave Session States

TRANSPORT LAYER

- Defines the concept of request-response = transaction.
- Defines the concept of dialog
- Defines a method for acknowledging single and group requests (end to end connection and reliability).
- It provides the toolkit for minimizing the usage of D7AAdvP through requester-controlled ad-hoc extension of the foreground scan.

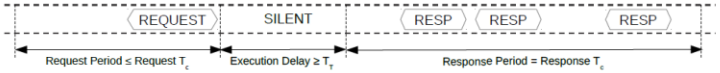


Figure 8.1.1.1: D7ATP Broadcast Transaction

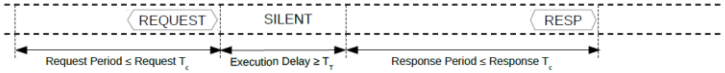


Figure 8.1.1.2: D7ATP Unicast Transaction

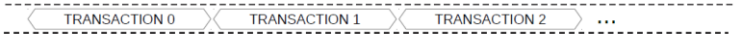


Figure 8.1.4.1: D7ATP Dialog

DLL	NW	Transport Layer							NW	DLL
Header	Header	CTRL	Dialog ID	Trans. ID	AGC	T_L	T_E	T_C	Payload	Footer	Footer
		1 byte	1 byte	1 byte	0/1 byte	0/1 byte	0/1 byte	0/1 byte	0-239 byte		

Table 8.2.1: D7ATP Request Segment Structure

DLL	NW	Transport Layer								NW	DLL
Header	Header	CTRL	Dialog ID	Trans. ID	AGC	T_L	T_E	Acknowledge Template	Payload	Footer	Footer
		1 byte	1 byte	1 byte	0/1 byte	0/1 byte	0/1 byte	0-34 byte	0-239 byte		

Table 8.2.2: D7ATP Response Segment Structure

NETWORK LAYER

- Authentication and Encryption options based on well established security algorithms:
- AES 128 bits CTR/CBC-MAC/CCM algorithms
- Native Support for No-Hop & One-Hop. Hopping remains compatible with security.
- Can be extended for multi-hop.

DLL	*D7ANP Network Layer*								*DLL*
Header	**Control**	**Origin XCL + ID**	**Hopping Control**	**Hopping XCL + ID**	**Hopping T_L**	**Security Header**	**Payload**	**Security Footer**	**Footer**
	1 byte	1/2/3/9 bytes	1 byte	1/2/3/9 byte	1 byte	0/5 bytes	0-250 bytes	0-16 bytes	
			Optional			Optional		Optional	
	Protectable					Protectable	Encryptable		

Table 7.3.1.1: *D7ANP* Frame Structure

DLL	*D7AAdvP*	*DLL*
Header	***ETA***	**Footer**
	2 bytes (Ti)	

Table 7.2.1.1: D7AAdvP Frame Structure

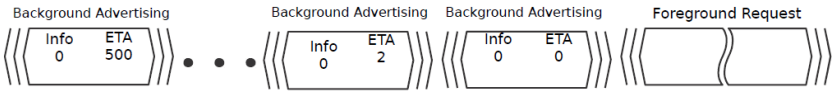


Figure 7.2.2.1: Example of flooding advertising frames prior to request

DATA LINK LAYER

- Provides the air-link toolkit : channel scan, reception, transmission, medium multiple access (CSMA-CA).
- The access to the medium is performed using a mandatory listen-before-talk routine.
- First level of frame filtering (subnet, link quality, address)
- Access Profile = channel(s) scanned during scan automation, type of scan, sleep period, Tx EIRP, etc...

PHY Header	Length	Subnet	CTRL	TADR	Payload	CRC16	PHY Footer
	1 Byte	1 byte	1 byte	0/1/2/8 bytes	0-251 Bytes	2 Bytes	

Table 6.3.1: Data Link Foreground Frame Structure

PHY Header	Subnet	CTRL	Payload	CRC16	PHY Footer
	1 byte	1 byte	2 Bytes	2 Bytes	

Table 6.3.3: Data Link Background Frame Structure

DATA LINK LAYER

CSMA-CA

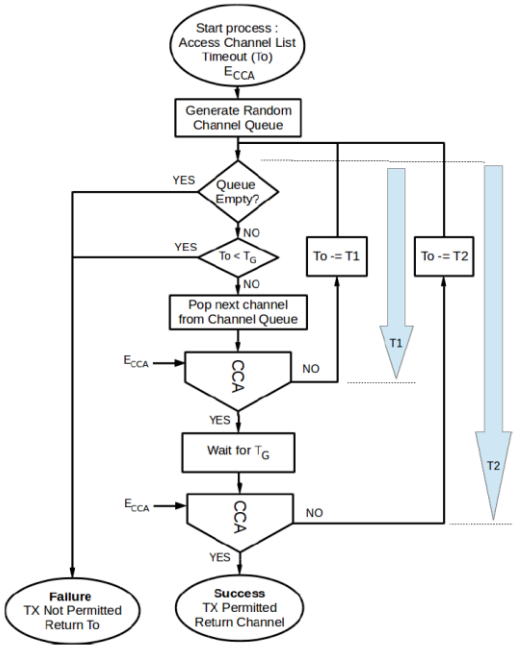


Figure 6.8.3.1: CSMA Process

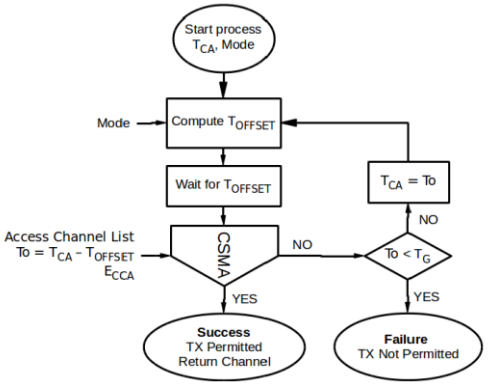


Figure 6.8.4.1: CSMA-CA Process

Mode	Index	Description
UNC	0	**Unconditional Transmission.** Transmission is permitted unconditionally on any channel of Access Channel List for a period not longer than T_{CA} with minimum silence period T_T.
AIND	1	**Adaptive Increase No Division.** Initial insertion, Adaptive (length-based) slotting, linear slot back-off. Ad-hoc slotting takes place, the insertion happens at the beginning of the slot, and the slot duration is equal to T_{TX}. On every insertion a CSMA process is executed. If it fails, a random wait duration, multiple of the slot duration, is applied before engaging the next insertion. The random wait value is limited to: 0 < random wait < T_{CA}.
RAIND	2	**Random Adaptive Increase No Division.** Random insertion, Adaptive (length-based) slotting, linear slot back-off. Identical to AIND, except that on initialization a random wait duration is applied before engaging the CSMA Process. The random wait value is limited to: 0 < random wait < T_{CA}.
RIGD	3	**Random Increase Geometric Division.** Random Increase, geometric decaying slot back-off. Ad-hoc slotting takes place, the slot insertion is random, and the slot duration decays by the model $(T_{CA0})(1 / 2^{(n+1)})$, where n ≥ 0 and T_{CA0} is the duration of the timeout for all slots.
RFU	4-15	Reserved for Future Use

Table 6.8.4.2: CSMA-CA Flow and Congestion Process Models

DATA LINK LAYER

ACCESS PROFILES

- Group all the Access parameters into an Access Profile
- Profiles are stored in dedicated D7A files. Maximum 15 profiles are allowed in the network.
- Each profile is referred to by its index called Access Class.
- Access Profiles are generally not transmitted over the air, they are configured by the Network Manager.
- A device transmits its Access Class to the device it is communicating with.

Parameter	Size	Description
CH	1 byte	Channel Header (5.3)
SP[4]	4x2 bytes	Subprofiles 0 to 3 (6.5.1.2)
SB[8]	8x7 bytes	Subbands 0 to 7

Table 6.5.1.1: Access Profile

Subband Bitmap	**1 byte**	Bitmap of used subbands
T_{SCHED}	1 byte	Scan automation period (compressed format)

*Table 6.5.1.2: **Access Sub-Profile***

PHYSICAL LAYER

- Defines the spectrum, modulation and channel coding characteristics
- Capable of performing RSSI measurement with 6 dBm accuracy.
- Programmable output power for AGC
- Automatic low-power RX polling
- Automatic CCA before transmitting (listen-before-talk)

ISM Band	ISM Band Index	Start (MHz)	End (MHz)
RFU	0x0-0x1		
433 MHz	0x2	433.060	434.785
868 MHz	0x3	863.000	870.000
915 MHz	0x4	902.000	928.000
RFU	0x5-0x7		

Table 5.1.1.1: Channel Bands

Channel Class	Index	Channel Spacing (MHz)	Modulation	Symbol Rate (kbps)	Modulation Index	Symbol 0	Symbol 1
Lo-Rate	0x0	0.025	2-(G)FSK	9.6	1	F(B,I) – 4.800 KHz	F(B,I) + 4.800 KHz
RFU	0x1						
Normal	0x2	0.200	2-(G)FSK	55.555	1.8	F(B,I) – 50.000 KHz	F(B,I) + 50.000 KHz
Hi-Rate	0x3	0.200	2-(G)FSK	166.667	0.5	F(B,I) – 41.667 KHz	F(B,I) + 41.667 KHz

Table 5.1.3.1: Modulation Schemes

ISM Band	Lo-Rate	Normal & Hi-Rate
433 MHz (*)	0, 1, …, 68	0, 8, 16, …, 56
868 MHz (**)	0, 1, …, 279	0, 8, 16, …, 216, 229, 239, 257, 270
915 MHz (***)	0, 1, …, 1039	0, 8, 16, …, 1032

Table 5.1.2.1: Allowed Channel Indexes

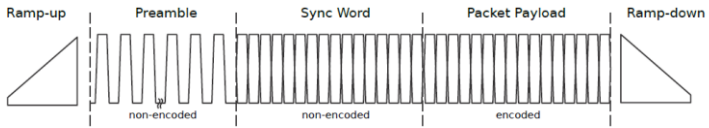
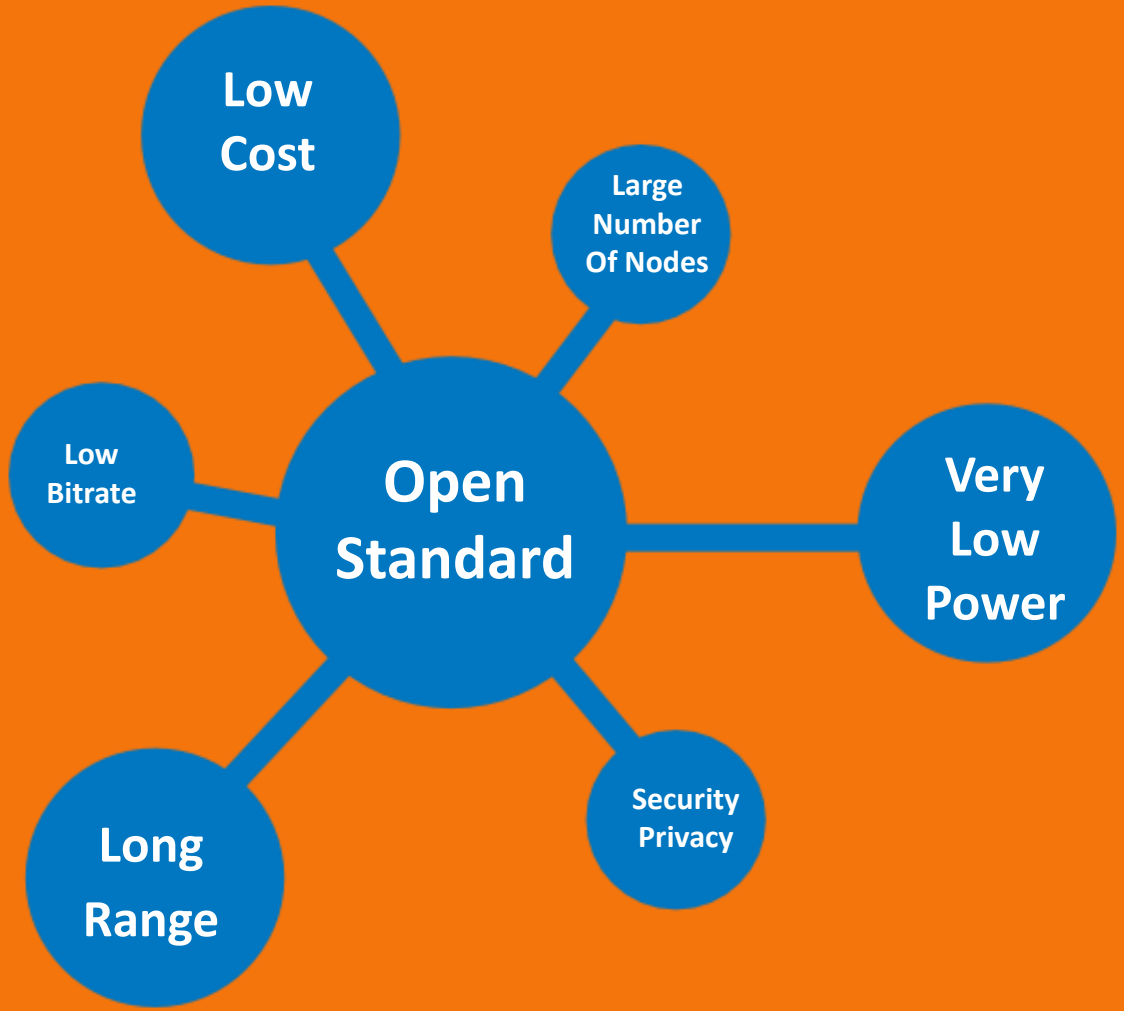


Figure 5.6.1.1: General structure for all packets.

OSS7 PROTOCOL STACK

- OSS-7 is an open source implementation of the DASH7 Alliance protocol
- Reference implementation for spec
- Code readability more important than performance
- HAL API allows support multiple platforms
- (MCU, radios, ...)
- Code hosted on github: https://github.com/MOSAIC-LoPoW/dash7-ap-open-source-stack


Low Cost
Large Number Of Nodes
Low Bitrate
Open Standard
Very Low Power
Long Range
Security Privacy