Wi-Fi Aware™ Specification

Version 4.0

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

This document may be used with the permission of Wi-Fi Alliance under the terms set forth herein.

By your use of the document, you are agreeing to these terms. Unless this document is clearly designated as an approved specification, this document is a work in process and is not an approved Wi-Fi Alliance specification. This document is subject to revision or removal at any time without notice. Information contained in this document may be used at your sole risk. Wi-Fi Alliance assumes no responsibility for errors or omissions in this document. This copyright permission does not constitute an endorsement of the products or services. Wi-Fi Alliance trademarks and certification marks may not be used unless specifically allowed by Wi-Fi Alliance.

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance's copyright.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY WI-FI ALLIANCE AND WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT.

Document revision history

Version	Date YYYY-MM-DD	Remarks
0.0.24	2014-12-11	Public draft release.
1.0	2015-05-01	Public release version.
2.0	2017-10-20	Added features for Release 2.
3.0	2018-12-10	Added features for Release 3.
3.1	2020-01-15	Added NFC Triggered NAN operations
3.2	2020-10-23	Editorial update
4.0	2022-12-07	Added features for Release 4.

Table of contents

List of tables

List of figures

1 Introduction

This document is the specification for Wi-Fi CERTIFIED Wi-Fi Aware™. This specification defines architecture, protocols, and functionality for interoperability of Wi-Fi Aware™-certified devices. The term *NAN* found throughout this document is interchangeable with *Wi-Fi Aware*.

1.1 Scope

The scope of the feature requirements is limited to that defined in this specification. The content of this specification is designed to address the solution requirement areas including user experience as identified below:

- MAC with NAN support
- Discovery Engine support
- Discovery Engine Application interface
- Discovery Engine Protocol and functionality
- NAN Data Engine
- NAN Data Engine Application interface
- NAN Data Engine Protocol and functionality
- Ranging Application interface
- Ranging Protocol and functionality
- NAN Scheduler Protocol and functionality

1.2 References

Knowledge of the documents listed in this section is required for understanding this specification. If a reference includes a date or a version identifier, only that specific version of the document is required. If the listing includes neither a date nor a version identifier, then the latest version of the document is required. In the event of a conflict between this specification and the following referenced documents, the contents of this specification take precedence.

[1] IEEE Computer Society, “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,” (IEEE Std. 802.11™-2022)

[2] IEEE Computer Society, “IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture,” (IEEE Std. 802®-2014), https://standards.ieee.org/findstds/standard/802-2014.html

[3] Wi-Fi Alliance®, "Wi-Fi Peer-to-Peer Services Technical Specification", https://www.wi-fi.org/discover-wi-fi/specifications

[4] Wi-Fi Alliance®, “Wi-Fi Multimedia Technical Specification, Version 1.2”, 2012, https://www.wi-fi.org/discover-wi-fi/specifications

[5] University of California, Davis “The SIV Mode of Operation for Deterministic Authenticated-Encryption (Key Wrap) and Misuse-Resistant Nonce-Based Authenticated-Encryption”, Draft 0.32, 2007, http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/siv/siv.pdf

[6] Internet Open Source, Apple, Inc., “CRC32.c”, http://www.opensource.apple.com/source/xnu/xnu-1456.1.26/bsd/libkern/crc32.c

[7] IETF RFC 4291, "IP Version 6 Addressing Architecture", https://www.ietf.org/rfc/rfc4291.txt

[8] IETF RFC 8018, "PKCS #5: Password-Based Cryptography Specification", https://tools.ietf.org/html/rfc8018

[9] Wi-Fi Alliance®, "Wi-Fi Aware Recommended Practices for Conveying DNS-SD Records", https://www.wi-fi.org/discover-wi-fi/wi-fi-aware

[10] IETF RFC 7217, "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", https://tools.ietf.org/html/rfc7217

[11] Internet Assigned Numbers Authority (IANA): https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

[12] IETF RFC 6763, "DNS-Based Service Discovery", https://tools.ietf.org/html/rfc6763

[13] Bluetooth Special Interest Group, “Transport Discovery Service”, November 2015, https://www.bluetooth.org/en-us/specification/adoptedspecifications

[14] IETF RFC 5234, "Augmented BNF for Syntax Specifications: ABNF", https://tools.ietf.org/html/rfc5234

[15] IETF RFC 6335, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", https://tools.ietf.org/html/rfc6335

[16] SipHash, https://131002.net/siphash

[17] NFC Forum, "Connection Handover (CH) Technical Specification 1.5", https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/specification-releases/

[18] IETF RFC 8110, " Opportunistic Wireless Encryption", https://tools.ietf.org/html/rfc8110

[19] IEEE Draft Standard P802.11-REVme™/D1.0, December 2021

[20] P802.11az™, D4.0

[21] WPA3 Specification, Version 3.0

1.3 Definitions and acronyms

1.3.1 Shall/should/may/might word usage

The words shall, should, and may are used intentionally throughout this document to identify the requirements for the NAN program.

The word shall indicates a mandatory requirement. All mandatory requirements must be implemented to assure interoperability with other Multiband Operations products.

The word should denotes a recommended approach or action.

The word may indicates a permitted approach or action with no implied preference.

The word might indicates a possibility or suggestion.

1.3.2 Conventions

The ordering of bits and bytes in the fields within information elements, attributes and action frames shall follow the conventions in section 9.2.2 of [1] unless otherwise stated.

The word ignored shall be used to describe bits, bytes, fields or parameters whose values are not verified by the recipient.

The word reserved shall be used to describe objects (bits, bytes, or fields or their assigned values) whose usage and interpretation will be defined in the future by this specification or by other technical specifications/bulletins. A reserved object shall be set to zero unless otherwise stated. The recipient of a reserved object shall ignore its value unless that object becomes defined at a later date. The sender of an object defined by this specification shall not use a reserved code value.

1.3.3 Definitions

The definitions in Table 1 are applicable to this specification.

Table 1. Definitions

Term	Definition
Cipher Suite	A bundle of algorithms and parameters that fully define a profile for security related processing. The Cipher Suite provides a means for protocols to support cryptographic agility and version changes in the security processing. The Cipher Suite is identified by a Cipher Suite Identifier.
Cipher Suite Identifier	An octet string representing a specific Cipher Suite. The Cipher Suite Identifier octet string shall be at least 1 and no more than 32 octets in length. Single octet Cipher Suite Identifier values are defined to ensure uniqueness for well-known suites of algorithms. Longer Cipher Suite Identifier values are allowed to support the creation of unique values using hashes.
Committed Further Availability Window	A Further Availability Window that a NAN Device commits to be available to receive and transmit NAN frames.
Common Resource Block	A set of synchronized NAN Slots outside the Discovery Windows that are contiguous in time domain, are in the same channel, are shared by two or more NAN Devices to receive and transmit NAN frames between each other.
Conditional Further Availability Window	A Further Availability Window that a NAN Device proposes during schedule negotiation, and becomes committed upon successfully completing the schedule negotiation.
Further Availability Window	A set of NAN Slots outside the Discovery Windows that are contiguous in time domain and are associated with the same channel or channel set, and are advertised by a NAN Device to be available to receive and transmit NAN frames.
Immutable Resource Block	Resource Blocks a NAN Device proposes during NAN Device Link schedule negotiation, and expects the peer NAN Device to fully accept without any change.
NAN Beacon	A NAN Beacon includes of all NAN Discovery Beacon and NAN Synchronization Beacon frames.
NAN Cluster	A collection of NAN devices that are synchronized to the same Discovery Window schedule.
NAN Concurrent Device	A NAN Device that is capable of operating in a NAN network and other types of Wi-Fi networks such as WLAN infrastructure, IBSS, and Wi-Fi Direct.
NAN Device	Any device that implements the NAN protocol.
NAN Discovery Beacon	A modified IEEE 802.11 Beacon management frame transmitted outside NAN Discovery Windows to facilitate discovery of NAN Clusters.
NAN Discovery Channel	The 2.4 GHz channel, and optionally a 5 GHz channel, on which NAN Discovery operations occur.
NAN Discovery Engine	The part of the NAN stack that implements the Publish and Subscribe mechanisms.
NAN Discovery Window	The time and channel on which NAN Devices converge.
NAN ID	An identifier signifying a specific set of NAN parameters.
NAN Infrastructure Device	A NAN Device whose default Master Preference setting is greater than or equal to 128 and intends to be a NAN Master Device.
NAN Network	A collection of NAN Clusters that share the same NAN ID.
NAN Security Group	Two or more NAN Devices that share a common security policy and compatible security credentials or keying material for one or more service such that any member may send encrypted unicast frames to any other member of the group.
NAN Synchronization Beacon	A modified IEEE 802.11 Beacon management frame transmitted inside NAN Discovery Windows used for NAN timing synchronization.
NAN Data Cluster	Collection of NAN Device Links with the same NAN Data Cluster Base schedule
NAN Device Link	The negotiated Resource Blocks between a pair of NAN Devices used for NAN operations.
NAN Data Path	The data connection established between a pair of NAN Devices for a service instance.

Term	Definition
NDC Schedule	A set of Resource Blocks when NAN devices in the same NAN Data Cluster are awake.
Publish	A mechanism for an application on a NAN Device to make selected information about the applications capabilities and services available to other NAN devices.
Synchronized NAN Device Link	The NAN Device Link.
NAN Slot	A radio resource unit with length of 16 TU in time domain, and the beginning of the first NAN Slot aligned with time zero.
Potential Further Availability Window	A Further Availability Window that a NAN Device prefers to be available to receive and transmit NAN frames, if needed
Unaligned Window	An availability or unavailability window that is contiguous in time domain, and unaligned with the boundaries of NAN Slots.
Notification	A mechanism for the NAN stack to inform the application on an event matching criteria given either in Publish or Subscribe.
Robust Security Network Association	As defined in [1]
Secure Service ID	A Service ID used by a NAN Security Group for discovery of peers publishing or subscribing to a protected service. A NAN Security Group may support multiple Secure Service IDs.
Security Context ID	An octet string representing the security policy and parameters used by a NAN Security Group. The security context ID defines algorithms and parameters used for processing messages within a context of secure communication. These parameters assist in establishing a pair-wise security association and associated symmetric keys. For a symmetric key establishment method, the Security Context Identifier identifies the shared key (similar to an 802.11 PMKID).
Security Association	A set of shared attributes between network entities to support secure communication. A security association may include attributes such as: cryptographic algorithm and mode; traffic encryption key.
Service ID	The first 48 bits of the SHA-256 hash of the Service Name. A lower-case representation of the Service Name shall be used to calculate the Service ID.
Service Name	A string uniquely identifying the service. The designer of the service selects the name and ensures that it is unique for the service. The Service Name is a UTF-8 encoded string from 1 to 255 bytes in length. The only acceptable single-byte UTF-8 symbols for a Service Name are alphanumeric values (A-Z, a-z, 0-9), the hyphen ('-'), the underscore ('_'), and the period ('.'). All valid multi-byte UTF-8 characters are acceptable in a Service Name. String matching performed on a Service Name should be case insensitive by converting the single byte values [A-Z] to lower-case before any processing.
Sub Slot Schedule	A refinement of Committed Further Availability Window that specifies the time intervals (Sub Slots) in the Committed window during which the device commits to be available to transmit and receive NAN frames.
Subscribe	A mechanism for an application user to gather selected types of information about capabilities and services of other NAN Devices.
Synchronized NAN Device Link	A NAN Device Link type.
Unaligned Window	An availability or unavailability window that is contiguous in time domain, and unaligned with the boundaries of NAN Slots.

1.3.4 Abbreviations and acronyms

Table 2 defines the acronyms used throughout this document. Some acronyms are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance.

Table 2. Abbreviations and acronyms

Acronyms	Definition
AC_VO	WMM Access Category - Voice
AFC	Automated Frequency Coordination
AMP	Anchor Master Preference
AMBTT	Anchor Master Beacon Transmission Time
AMR	Anchor Master Rank
AP	Access Point
ASI	Aligned Schedule Indication
ASP	Application Service Platform
BIGTK	Beacon Integrity Group Transient Key used to protect Beacon frames
BSSID	Basic Service Set Identifier
C2C	Client to Client
CEPT	Conference of European Postal & Telecommunications
CG	Cluster Grade
CW	Contention Window
CRB	Common Resource Block
CRS	Committed Ranging Schedule
CSIA	Cipher Suite Information attribute
CSID	Cipher Suite Identifier
DE	Discovery Engine
DCEA	Device Capability Extension attribute
DFS	Dynamic Frequency Selection
DW	Discovery Window
EDCA	Enhanced Distributed Channel Access
FA	Further Availability
FAW	Further Availability Window
FSD	Further Service Discovery
FTM	Fine Time Measurement
IBSS	Independent Basic Service Set
ID	Identifier
IE	Information Element
IGTK	Integrity Group Transient Key used to protect multicast management frames
GHz	Giga Hertz

Acronyms	Definition
GTK	Group Transient Key used to protect group addressed data frames
HC	Hop Count
KDF	Key derivation function
LPI	Low Power Indoor
LSB	Least Significant Bit
MAC	Medium Access Control
Mbps	Megabits per second
MF	Matching Filter
MME	Management MIC element
MP	Master Preference
NAF	NAN Action Frame
NDC	NAN Data Cluster
NDI	NAN Data Interface address
NDL	NAN Device Link
NDP	NAN Data Path
NDPE	NDP Extension
ND-TKSA	NAN Data Pairwise Security Association
NIK	NAN Identity Key
NIRA	NAN Identity Resolution attribute
NMF	NAN Management frame
NMI	NAN Management Interface address
ND-TKSA	NAN Data Pairwise Security Association
NIK	NAN Identity Key
NIRA	NAN Identity Resolution attribute
OFDM	Orthogonal Frequency Division Multiplexing
OUI	Organizationally Unique Identifier
P2P	Peer-to-Peer
P2Ps	Peer-to-Peer services
PASN	Preassociation Security Negotiation
P-NDL	Paged NAN Device Link
PN	Packet Number
RSNA	Robust Security Network Association
S-NDL	Synchronized NAN Device Link
SA	Security Association
SCIA	Security Context Information Attribute
SCID	Security Context Identifier

Acronyms	Definition
SD	Service Discovery
SDA	Service Descriptor Attribute
SDEA	Service Descriptor Extension attribute
SDF	Service Discovery frame
SID	Service ID
SKDA	Shared Key Descriptor attribute
SP	Standard Power
SRD	Specification Requirements Document
SRF	Service Response Filter
SSID	Service Set Identifier
STA	Station
TB	Time Block
TBTT	Target beacon transmission time
TDLS	Tunneled Direct Link Setup
TPEA	Transmit Power Envelope attribute
TSF	Time Synchronization Function
TUs	Time Units
TxW	Transmission Window
ULW	Unaligned Window
USD	Unsynchronized Service Discovery
VLP	Very Low Power
WLAN	Wireless Local Area Network
WMM®	Wi-Fi Multimedia™

2 NAN Architecture

2.1 NAN components

The NAN architecture consists of components that interact to support the NAN communication protocol.

A NAN Device:

- Shall support both NAN Non-Master and NAN Master role
- Shall support NAN Master Selection procedure for role and state definition
- Shall support all required NAN protocol mechanisms
- May support concurrent operation in NAN and other types of Wi-Fi networks

2.2 NAN cluster topology

A NAN Network comprises all NAN Devices that share a common set of NAN parameters that include: the time period between consecutive Discovery Windows, the time duration of the Discovery Windows, the beacon interval, and NAN Discovery Channel(s).

A NAN Cluster is a collection of NAN devices that share a common set of NAN parameters and are synchronized to the same Discovery Window schedule. A NAN Cluster is identified by the NAN Cluster ID described in section 9.

A representation of a NAN Cluster is illustrated in Figure 1.

A NAN Device may send multicast NAN Service Discovery frames directly to other NAN devices within range in the same NAN Cluster during the Discovery Window. A NAN Device may send unicast NAN Service Discovery frames directly to any other NAN Device within range in the same NAN Cluster during the Discovery Window.

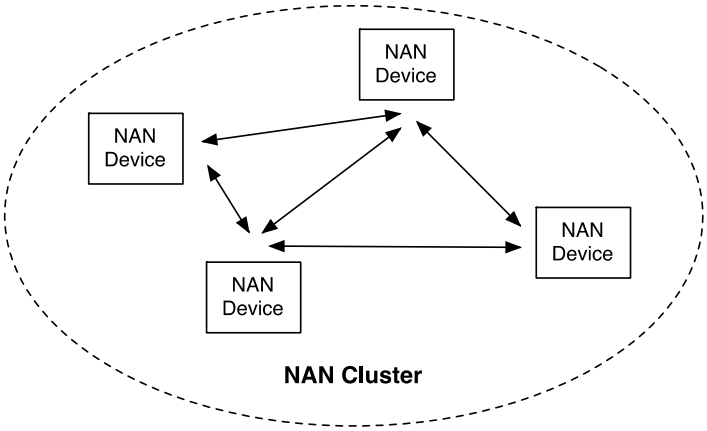


Figure 1. NAN cluster

NAN Devices that are part of the same NAN Cluster participate in the NAN Master Selection procedure. NAN Master Selection is performed on a NAN Cluster basis. Depending on changes in the NAN Cluster, such as NAN Devices that are part of NAN Cluster and their Master Ranks, different NAN Devices may be elected to become NAN Devices in Master role at different times as illustrated in Figure 2. NAN Devices with equal Master Preference (refer to section 3.3.3) will have equal chance of becoming a NAN Master.

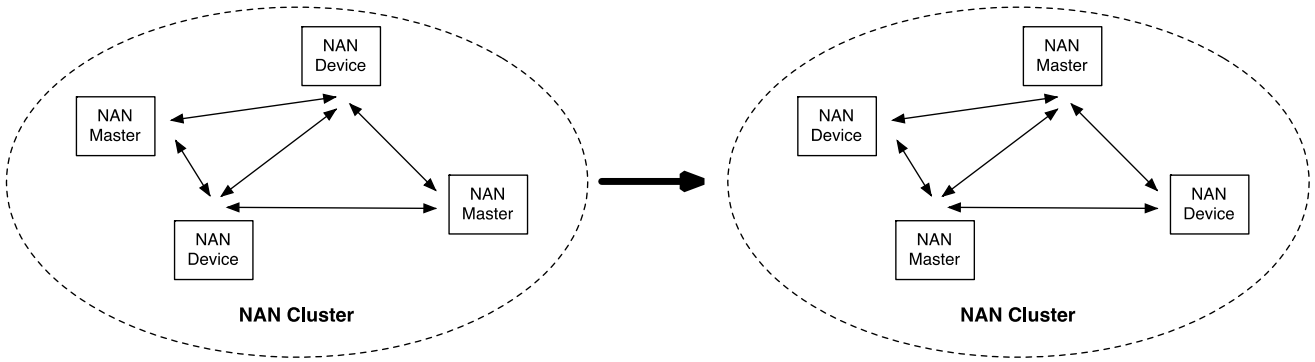


Figure 2. NAN cluster with alternating master devices

Figure 3 illustrates a NAN Network with two overlapping NAN Clusters. At any given time, a NAN Device may be within range of more than one NAN Cluster that can be discovered using passive scanning. Such a NAN Device may choose to synchronize with one or more NAN Clusters. Alternatively, the two NAN Clusters may merge as NAN Devices in one NAN Cluster discover the existence of the other NAN Clusters and converge into a common NAN Cluster.

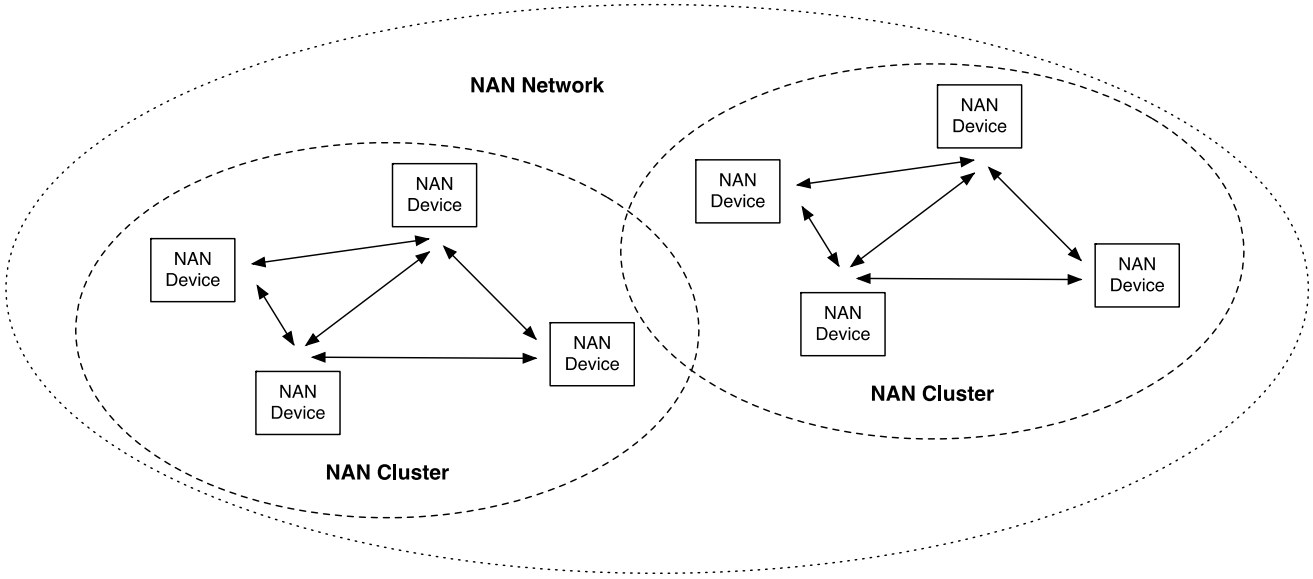


Figure 3. NAN Network with overlapping NAN Clusters

As shown in Figure 4, a NAN Device may choose to participate in more than one NAN Cluster, e.g. to quickly discover all services offered by the NAN Devices of all NAN Clusters within range. The details of such concurrent NAN Cluster operation are implementation specific, however such operation is optional or out of scope and therefore not described in this specification. Note that a NAN Device that chooses to participate in a NAN Cluster by sending NAN Service Discovery frames shall also participate in the NAN Master Selection procedure for transmission of NAN Synchronization and NAN Discovery Beacon frames for that NAN Cluster.

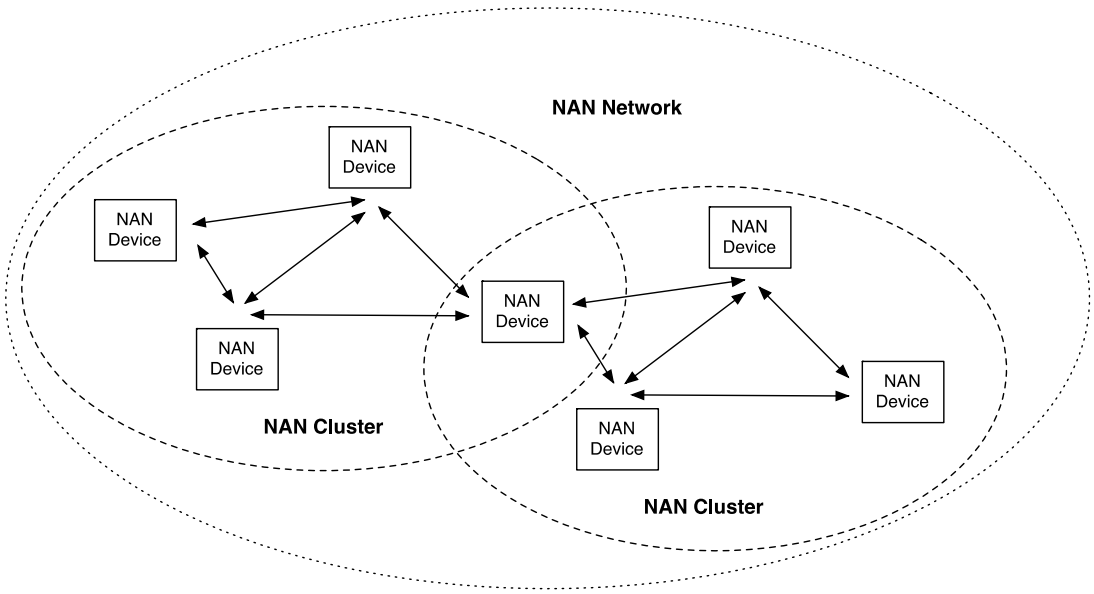


Figure 4. NAN Network with overlapping NAN Clusters with a NAN Device participating in both NAN Clusters

2.3 NAN data communication architecture

2.3.1 Unicast support

To initiate a unicast data communication between a NAN Device pair, a service requests to set up a NAN Data Path (NDP). The NAN Device pair establishes a NAN Device Link (NDL) to ensure that they share sufficient NDL Common Resource Blocks (CRBs) to accommodate the NDP. Once an NDL is established, it can be updated to support more NDPs between the NAN Device pair.

A NAN Data Cluster (NDC) consists of two or more NAN Devices in the same NAN Cluster that share a common NDC Schedule identifying when each NAN Device is awake. Each member device in the NDC has at least one NDL with another member device within the same NDC. An example of a NDP, NDL, and NDC is shown in Figure 5.

A NAN Device can be a member of more than one NDC, while an NDL belongs to exactly one NDC.

In an NDC, all member NAN Devices maintain synchronization amongst each other and are present at the same NDC CRBs indicated by the NDC Schedule.

Each NDL has its own NDL Schedule. The NDL Schedule is a superset of the NDC Schedule.

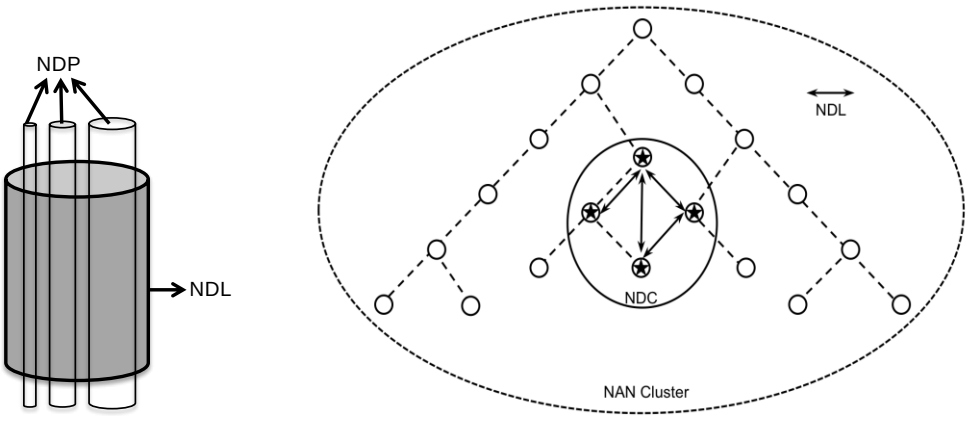


Figure 5. NDP, NDL, and NDC example

2.4 NAN ranging architecture

NAN ranging functionality allows devices to determine the distance between two NAN Devices in a NAN cluster as shown in Figure 6. To execute the NAN Ranging operation, NAN Devices shall set up one or more time-blocks to execute the distance measurement protocol. The distance estimate is produced using the Fine Time Measurement (FTM) protocol that is described in [1].

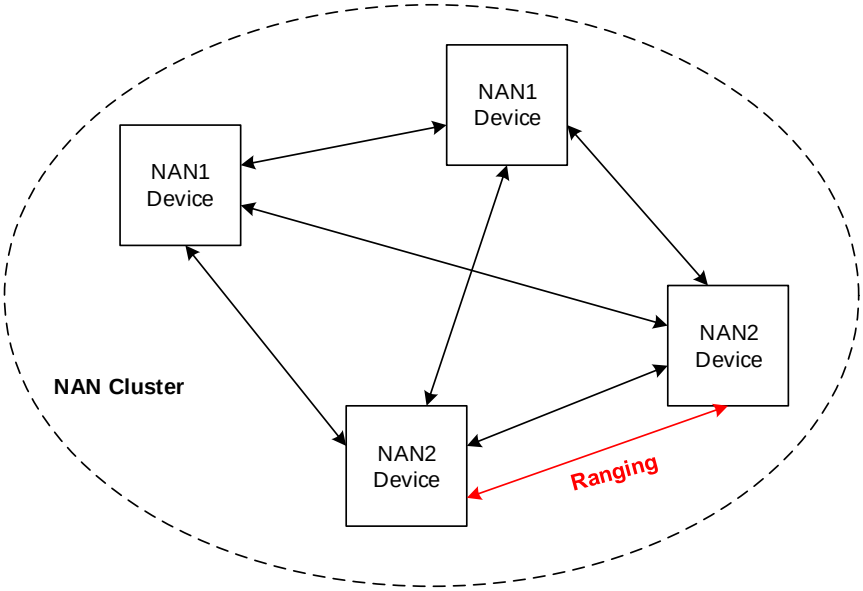


Figure 6. NAN cluster with two NAN devices performing NAN ranging

2.5 NAN functional architecture

Figure 7 illustrates the high-level architecture and components in the NAN framework. The main components are the NAN Discovery Engine (DE), NAN Medium Access Control (MAC), and NAN APIs to services/applications.

Service queries and responses are processed by the NAN Discovery Engine. The NAN MAC component is responsible for processing and handling the NAN Beacon frames and NAN Service Discovery frames.

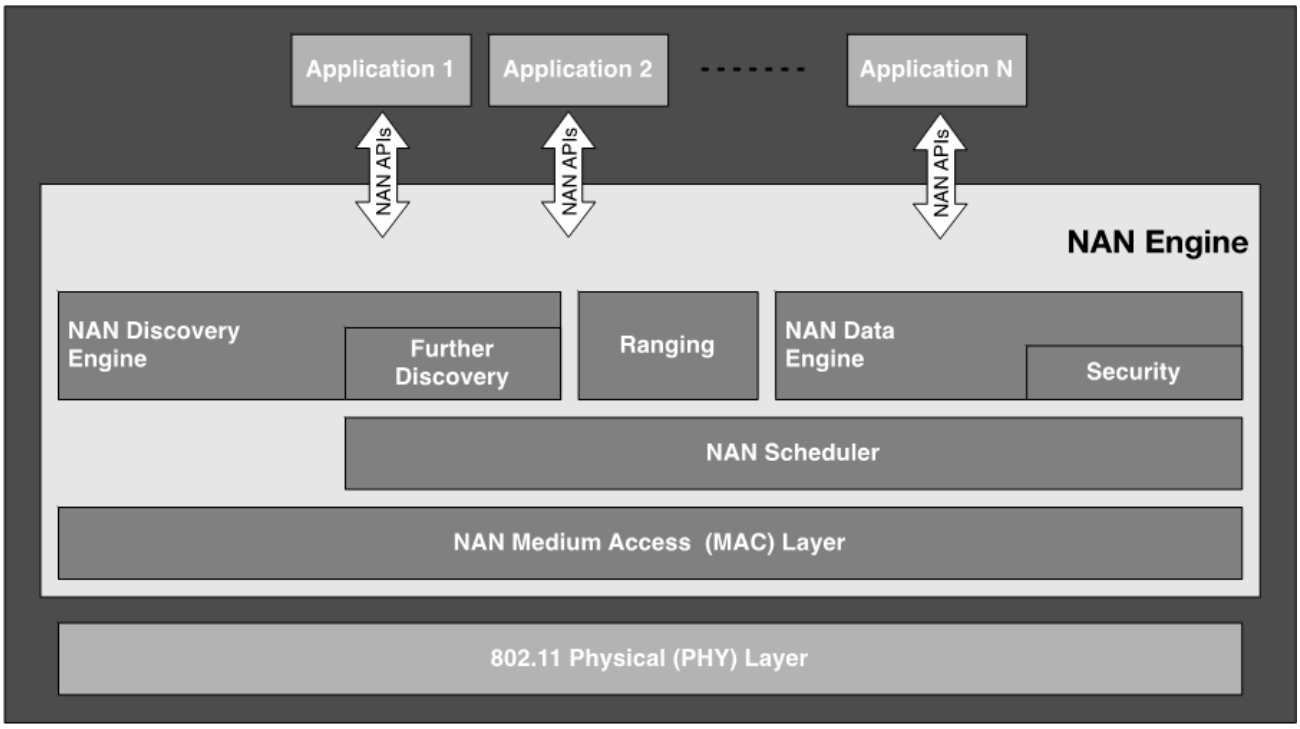


Figure 7. NAN functional architecture

NAN extends the service discovery function to include a mechanism for more detailed service discovery outside the Discovery Window. The NAN Engine encapsulates the NAN Discovery Engine, NAN Data Engine, Ranging, Scheduler, and the MAC functionality.

The NAN Data Engine provides the NAN Data Link capability (NDL) that is used to setup a data link between NAN Devices.

The NAN ranging component estimates the distance between NAN Devices that support the Ranging capability. Ranging may be used in addition to the service discovery mechanism to estimate the distance to a NAN Device providing a specific service.

2.6 Concurrent operation

A NAN Device may operate concurrently in a NAN network and in other types of Wi-Fi networks such as WLAN Infrastructure, IBSS, and/or Wi-Fi Direct. Such a device is considered a NAN Concurrent Device in this specification and is illustrated in Figure 8.

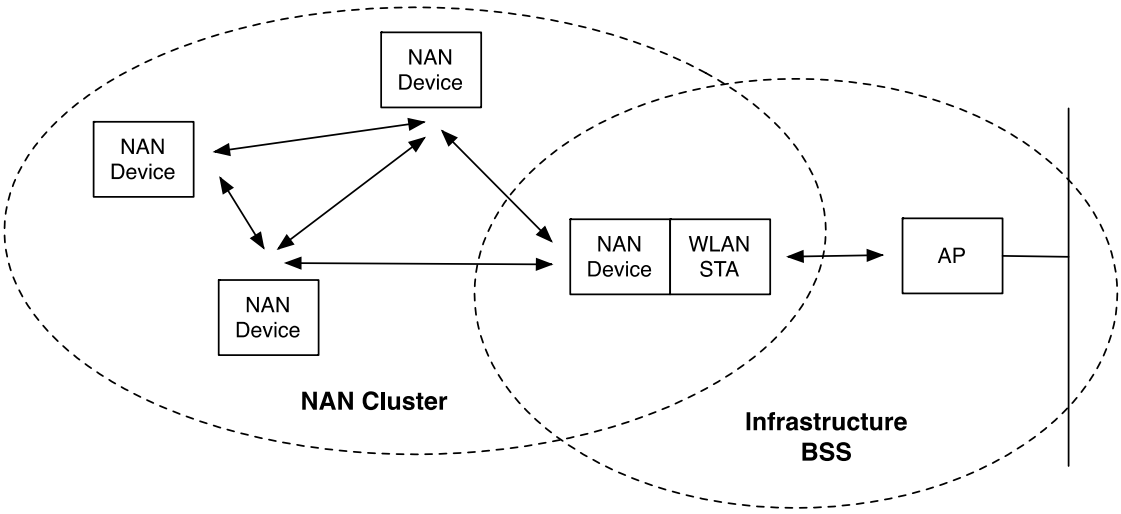


Figure 8. NAN device operating concurrently

A NAN Concurrent Device shall support multiple MAC entities: one MAC entity operating as a WLAN STA and the other MAC entity operating as a NAN Device. A NAN Device may operate as a member of a NAN network and WLAN Infrastructure network simultaneously, however, such operation is out of scope and therefore not described by this specification.

2.7 NAN Medium Access Control layer

The NAN MAC is responsible for obtaining and maintaining synchronization in the NAN Cluster that the NAN Device is operating in, by participating in the NAN Synchronization Beacon frame transmission as defined in section 3.3. As part of the synchronization function, the NAN MAC runs the TSF timer as defined in section 3.3.5. The NAN MAC is also responsible for transmitting NAN Discovery Beacon frames and conducting passive NAN discovery to find out available NAN Clusters as defined in section 3.3.8.

The NAN MAC provides frame transmit and receive services to the NAN Discovery Engine. The NAN MAC contends for access during the Discovery Window as defined in section 3.5.1 before transmitting a frame. The NAN MAC contends for access outside the Discovery Window as defined in section 3.6 before transmitting a frame.

2.8 NAN device addressing

A NAN Device shall maintain a NAN Management Interface Address (NMI) and may maintain one or more NAN Data Interface Addresses (NDIs), conforming to the format as described in section 9.2.4.3.2 of [1]. The NMI and NDI may be globally unique or locally administrated. An NDI may be the same as the NMI.

A NAN Device shall use the NMI or NDI as the transmitter address for all management frames sent within a NAN Cluster. A NAN Device shall use the NMI or NDI of the intended recipient NAN Device as the receiver address for all unicast management frames sent within a NAN Cluster, and shall use the broadcast address as the receiver address for management frames destined for all NAN Devices within a NAN Cluster. The usage of NMI or NDI for the transmitter address and receiver address for the management frames is described in Table 3.

A NAN Device may change its NMI. It is recommended that an NMI change be coordinated by specific services that need privacy. The rules on NMI changes are specified in section 7.5.

When a NAN Device sets up a NDP with a peer NAN Device, it shall select an NDI for the NDP. The NAN Device shall use the NDI as the transmitter address for all data frames associated with that NDP.

A NAN Device may use the same NDI for multiple different NDPs; or it may use different NDIs for different NDPs. For example, a NAN Device may use different NDIs for NDPs with different security requirements (refer to section 7.1).

A NDL is uniquely identified by the NMIs of the two NAN Devices that established the NDL. Figure 9 illustrates the use of NDIs and NMI within an NDL between two NAN Devices.

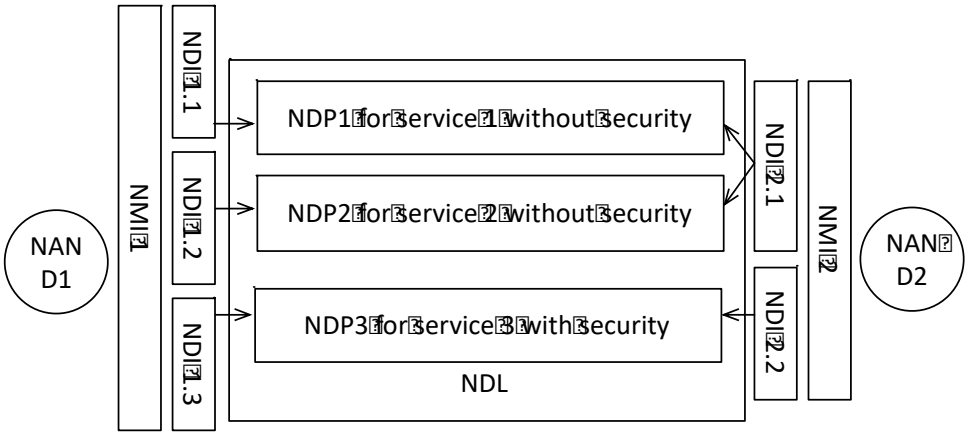


Figure 9. NDP, NDL, NMI, and NDI

2.8.1 NAN Network ID

The NAN Network ID is defined as the MAC address 51-6F-9A-01-00-00. Multicast NAN Service Discovery frames and NAN Action frames shall use the multicast address 51-6F-9A-01-00-00 in the A1 field.

2.8.2 NAN Cluster ID

The NAN Cluster ID is a MAC address that takes a value from 50-6F-9A-01-00-00 to 50-6F-9A-01-FF-FF and is carried in the A3 field of some of the NAN frames, as specified in Table 3. The NAN Cluster ID is randomly chosen by the device that initiates the NAN Cluster.

2.8.3 Address fields in NAN and Non-NAN frames

The setting of the toDS, fromDS, A1, A2 and A3 fields for the different frames in a NAN operations, except for the USD, are indicated in Table 3 and Table 4.

Table 3. Address field definition for NAN frames

Type	ToDS	FromDS	A1	A2	A3
NAN Beacon	0	0	Broadcast Address	NMI of sender	NAN Cluster ID
Multicast or unicast NAN SDF (Always sent without encryption)	0	0	NAN Network ID or NMI of receiver	NMI of sender	NAN Cluster ID
Multicast or Unicast NAN Action frame (unsecure)	0	0	NAN Network ID or NMI of receiver	NMI of sender	NAN Cluster ID
NDP Unicast Data frame	0	0	NDI of receiver	NDI of sender	NAN Cluster ID
Multicast Data frames1	0	0	Multicast Address	NDI of sender	NAN Cluster ID
Notes: 1. A NAN Device should transmit multicast data frames during NDC CRBs or other common NAN Slots when intended receivers are available.					

The Multicast Data frame may be transmitted as an individually (unicast) addressed A-MSDU with the format as specified in section 9.3.2.2 of [1] which includes the A-MSDU subframe headers' DA address set to the multicast address for the corresponding MSDUs. A-MSDU operation is specified in section 10.12 of [1]. A NAN Device shall be able to receive such A-MSDU frames.

A NAN Device may transmit unsecure multicast data frames. However, a receiving NAN Device may ignore unsecure multicast data frames based on device policy.

Table 4. Address Field Definition for Non-NAN Management Frames

Type	ToDS	FromDS	A1	A2	A3
Unicast Management frame (secure)	0	0	NDI of receiver	NDI of sender	Unspecified
Unicast Public Action frame (unsecure)1	0	0	NMI of receiver	NMI of Sender	Unspecified
Unicast Non-Public Action frame (unsecure)2	0	0	NDI of receiver	NDI of Sender	Unspecified
PASN Authentication frame (unsecure)	0	0	NMI of receiver	NMI of Sender	NAN Cluster ID
Multicast Public Action frame (unsecure)	0	0	NAN Network ID	NMI of Sender	Unspecified
Multicast Non-Public Action frame (unsecure)	0	0	NAN Network ID	NDI of Sender	Unspecified

Notes:

1. For example, FTM Request frame and FTM frame are Non-NAN Public Action frame and shall be transmitted or received via NMI.

2. For example, Block Ack action frames, QoS action frames and Radio Resource actions frames are Non-NAN Action frames and shall be transmitted or received via NDI.

The settings of the toDS, fromDS, A1, A2 and A3 fields for the different NAN SDFs in the USD are indicated in Table 5.

Table 5. Address field definition for NAN SDF frames in USD

Type	ToDS	FromDS	A1	A2	A3
Multicast NAN SDF Subscribe	0	0	NAN Network ID	NMI of sender	NAN Cluster ID
Unicast NAN SDF Publish	0	0	NMI of receiver	NMI of sender	NAN Cluster ID of receiver (copied from the received NAN SDF Subscribe)
Multicast NAN SDF Publish	0	0	NAN Network ID	NMI of sender	NAN Network ID
NAN SDF Follow-up	0	0	NMI of receiver	NMI of sender	NAN Cluster ID, when transmitted by Subscriber NAN Cluster ID of receiver, when transmitted by Publisher (copied from the NAN SDF Follow-up received from Subscriber)

2.9 Requirements

2.9.1 Baseline Wi-Fi Alliance certification prerequisites

A NAN Device shall pass the following Wi-Fi Alliance Certifications:

- 802.11n certification for 2.4 GHz (mandatory)
- 802.11n certification for 5 GHz (optional)
- 802.11ac certification for 5 GHz (optional)

2.9.2 NAN specific requirements

Additionally, a NAN Device shall support the following:

- Device Clock Accuracy
  - The clock accuracy of a NAN Device shall be +/-500 ppm or better over a temperature range of 0-80˚C
- Data Rates
  - Minimum OFDM data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps

  - NAN Synchronization and NAN Discovery Beacon frames shall be transmitted at 6 Mbps
  - NAN Service Discovery Public Action frames shall be transmitted using any of the mandatory OFDM data rates

- Ranging
  - A NAN ranging capable device shall be able to operate as an initiator and a responder for the FTM protocol (see section 11.24.6.2 of [1])
  - In a ranging operation initiated as part of service discovery, the subscribe device shall have the FTM initiator role

3 NAN Synchronization

3.1 Introduction

NAN provides a mechanism for devices to synchronize the time and channel on which they converge to facilitate the discovery of services that have been made discoverable on existing devices or new devices that enter the RF environment. The NAN synchronization procedure specifies a time window and limits the number of operating channels to decrease the discovery latency, power consumption, and medium occupancy that would otherwise occur. The NAN synchronization procedure is separate from the service discovery messaging.

The time period and channel on which NAN Devices converge is called the Discovery Window (DW), as illustrated in Figure 10. During the Discovery Window the NAN Devices are available with high probability for mutual discovery. During interim periods the devices may be asleep or involved with other activities, for example, communicating on other networks, possibly on a different channel.

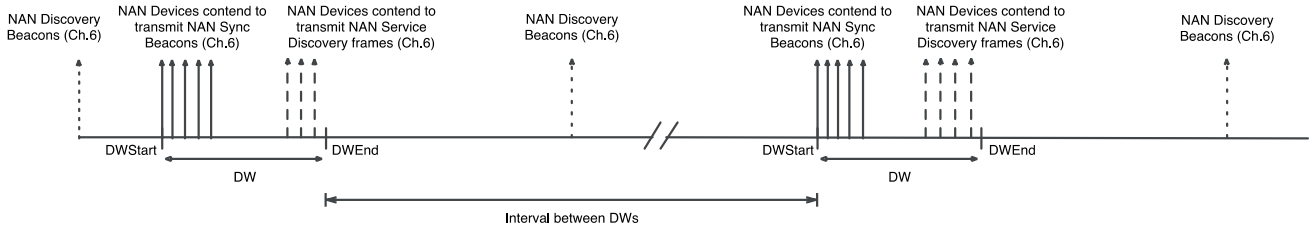


Figure 10. Discovery Window

3.2 Operating channels

NAN Discovery shall operate only in channel 6 (2.437 GHz) in the 2.4 GHz frequency band and may optionally operate in one channel in the 5 GHz frequency band. Other NAN operations may be performed in any channel.

If a NAN Device supports NAN Discovery operations in the 5 GHz frequency band, it shall support a NAN Discovery Channel in the 5 GHz frequency band. The specific NAN Discovery Channel in the 5 GHz frequency band is dependent on knowing the geographical location of the device and the applicable regulatory domain rules.

- If NAN Devices are permitted by local regulations to operate only in the 5.150 – 5.250 GHz Lower band (called UNII-1 by FCC, other names in other jurisdictions), the 5 GHz NAN Discovery Channel shall be channel 44 (5.220 GHz)
- If NAN Devices are permitted by local regulations to operate only in the 5.725 – 5.825 GHz Upper band (called UNII-3 by FCC, other names other jurisdictions), the 5 GHz NAN Discovery Channel shall be channel 149 (5.745 GHz)
- If NAN Devices are permitted by local regulations to operate in both the 5 GHz Lower and Upper bands, the 5 GHz NAN Discovery Channel shall be channel 149 (5.745 GHz)

Any other channel may be used for NAN Data Path operation if allowed by local regulations.

3.3 Synchronization of NAN Devices

NAN Devices participating in the same NAN Cluster are synchronized to a common clock. A TSF keeps the timers of all NAN Devices in the same NAN Cluster synchronized. The TSF in a NAN Cluster shall be implemented via a distributed algorithm performed by all NAN Devices. Each NAN Device participating in a NAN Cluster shall transmit NAN Beacon frames according to the algorithm described in this section.

3.3.1 NAN Discovery Window

A NAN Device that creates a NAN Cluster defines a series of Discovery Window Starting Times (DWSTs) exactly 512 TUs apart in the mandatory 2.4 GHz frequency band NAN Discovery Channel. For each NAN Device, time zero is defined to be the first DWST in the 2.4 GHz frequency band NAN Discovery Channel.

A NAN Device that also operates in 5 GHz frequency band shall define another series of DWSTs exactly 512 TUs apart in the 5 GHz frequency band NAN Discovery Channel. Time 128 TU is defined to be the first DWST in the 5 GHz frequency band NAN Discovery Channel.

As illustrated in Figure 10, a DW starts at each DWST and its duration shall be 16 TUs.

During a DW, one or more NAN Devices transmit NAN Synchronization Beacon frames such that all NAN Devices within the NAN Cluster synchronize their clocks. A NAN Device transmits at most one NAN Synchronization Beacon frame within one DW. The channel access rules used to transmit a NAN Synchronization Beacon frame are defined in section 3.5.1. A NAN Device may cancel a pending NAN Synchronization Beacon frame transmission according to the rules defined in section 3.3.6.5.

Between DWs, one or more NAN Devices shall transmit NAN Discovery Beacon frames to enable NAN Devices to discover the NAN Cluster. The NAN Discovery Beacon transmission rules are defined in section 3.3.6.5 and 3.3.8.1.

3.3.2 NAN Device Role and State

A NAN Device shall operate in either a Master role or a Non-Master role. When a NAN Device operates in a Non-Master role, it shall be in either a Non-Master Sync state or a Non-Master Non-Sync state. The NAN Device role and state transitions are defined in section 3.3.6.

A NAN Device in a Master role shall transmit both NAN Synchronization Beacon and NAN Discovery Beacon frames as specified in section 3.3.6.5.

A NAN Device in a Non-Master role and Sync state shall transmit NAN Synchronization Beacon frames within DWs as specified in section 3.3.6.5.

A NAN Device in a Non-Master role and Non-Sync state shall not transmit NAN Synchronization Beacon frames.

A NAN Device may transmit NAN Service Discovery frames within any DW, regardless of its role and state, according to the DW Contention Mitigation procedure in section 3.5.1.

All NAN Devices shall be awake during every DW0. DW0 is defined as the DW in which the lower 23 bits of the TSF are zero. DW0 is aligned with the start of DW in the 2.4 GHz irrespective of other bands that support NAN operation. A NAN Device in Non-Master Non-Sync state may choose to not be awake on the NAN Discovery Channels during other DWs.

3.3.3 NAN Master Rank

Each NAN Device maintains a NAN Master Rank, which represents a NAN Device’s grade to operate as NAN Master. The NAN Master Rank comprises of three components:

- Master Preference
- Random Factor
- NAN Interface Address

A higher numerical value of Master Preference means a NAN Device’s higher preference to serve as a NAN Master.

A NAN Device that activates the NAN functionality and starts a NAN Cluster shall set both the Master Preference and the Random Factor to zero in the Master Indication attribute, and shall initialize and reset the NANWarmUp timer. A NAN Device shall set the Master Preference field in the Master Indication attribute to a value greater than zero and shall initialize and set a new random value for the Random Factor field in the Master Indication attribute upon expiry of the NANWarmUp timer. The NANWarmUp timer value is 120 seconds.

If a NAN Device joins a NAN Cluster with the Anchor Master’s Master Preference greater than zero or its current NAN Cluster’s Anchor Master’s Master Preference value is changed to non-zero, the NAN Device shall set the Master Preference to a value greater than zero and shall set the Random Factor to a new random value, and cancel the NANWarmUp time.

If a NAN Device joins a NAN Cluster with the Anchor Master’s Master Preference equal to zero, the NAN Device should set the Master Preference to a value greater than zero, set the Random Factor to a new random value, and cancel the NANWarmUp timer.

If a NAN Infrastructure Device needs to set its Master Preference value greater than zero, either due to expiry of the NANWarmUp timer or due to joining a NAN Cluster with the Anchor Master's Master Preference greater than zero, it shall set its Master Preference to a value greater or equal to 128. All other NAN Devices shall set their Master Preference to a value smaller than 128. The Master Preference values of 1 and 255 are reserved for testing purposes only. A NAN Device shall consider 1 and 255 as valid Master Preference values but shall not use these values during normal operation.

Once a NAN Device sets a new Master Preference value that is greater than zero, it shall not change the Master Preference value until after 240 DWs, and shall not change the Master Preference value back to zero.

Once a NAN Device sets a new Random Factor value, it shall change the Random Factor value no later than 240 DWs, but not earlier than 120 DWs.

Each Random Factor value shall be a random integer between zero and 255 drawn from a uniform distribution.

Once a NAN Device changes its NAN Interface Address, it shall not change the NAN Interface Address again until after 240 DWs.

A NAN Device shall not change its Master Rank value within a DW.

The Master Rank of a NAN Device is calculated as follows:

Master Rank = Master Preference * 2^56 + Random Factor * 2^48 + MAC[5] *2^40 +… + MAC[0]

where MAC[0:5] is the NAN Interface Address using the octet number from Figure 10 of [2] (MAC[0] carries part of the OUI, Individual/Group bit and Universal/Local bit).

NOTE: As stated in the note on page 24 of [2], the upper bit stream representation in Figure 10 has the LSB of each octet on the left while the octet representation in the lower half of Figure 10 has the LSB in its usual position on the right.

A NAN Device that transmits a NAN Beacon frame shall include the Master Indication attribute in the NAN Beacon frame to indicate its Master Preference and Random Factor values.

3.3.4 Anchor Master

An Anchor Master is a NAN Device that has the highest Master Rank in a NAN Cluster. NAN Devices in a NAN Cluster follow the TSF of the Anchor Master. Each NAN Device shall be capable of operating as an Anchor Master. Each NAN Device operating in a NAN Cluster shall have an Anchor Master. On becoming an Anchor Master of an existing NAN Cluster, a NAN Device shall inherit the TSF being used in the existing NAN Cluster. NAN Devices operating in a NAN Cluster may temporarily have different Anchor Masters, but the rules and procedures specified in this section ensure that a NAN Cluster always converges to having one Anchor Master.

A NAN Device may become an Anchor Master in the following ways:

- Initially, upon starting a new NAN Cluster
- After a Master Rank change:
  - The NAN Device's own Master Rank changes
  - The Master Rank of another NAN Device in the same NAN Cluster changes
- NAN Beacon frames from the current Anchor Master of the NAN Cluster are no longer received

A NAN Device may lose its Anchor Master role when the NAN Device's own Master Rank changes, or when the Master Rank of another NAN Device in the NAN Cluster changes.

3.3.4.1 Anchor Master selection

Anchor Master Selection uses an algorithm to determine which NAN Device is the Anchor Master of the NAN Cluster. Each NAN Device shall run the Anchor Master Selection algorithm when participating in a NAN Cluster.

1. General Anchor Master Record rules for NAN Devices

A NAN Device shall save the Current Anchor Master Record that includes the following information about the NAN Device's Current Anchor Master:

- Anchor Master Rank (AMR): The Master Rank of the Anchor Master
- Hop Count to Anchor Master: the number of NAN Devices between the NAN Device and the Anchor Master.
- Anchor Master Beacon Transmission Time (AMBTT)

The Current Anchor Master Record shall be initialized as follows:

- The AMR is set to its own Master Rank
- The Hop Count to Anchor Master is set to zero
- The AMBTT is set to 0x00000000

In addition, a NAN Device shall save the Last Anchor Master Record that includes the following information about the NAN Device's previous Anchor Master:

- Anchor Master Rank (AMR)
- Anchor Master Beacon Transmission Time (AMBTT)

The Last Anchor Master Record shall be initialized to zero.

NOTE: When the NAN Device is operating as an Anchor Master, it does not use the Last Anchor Master Record.

2. Anchor Master Record rules for when a NAN Device becomes the Anchor Master

When a NAN Device becomes an Anchor Master it shall first set the information in its Last Anchor Master Record and then set the information in its Current Anchor Master Record as follows:

- The AMR in the Last Anchor Master Record shall be set to the corresponding value in the Current Anchor Master Record, except that, if the NAN Device has become an Anchor Master due to starting a new NAN Cluster, the AMR in the Last Anchor Master Record shall be set to its own Master Rank
- The AMBTT in the Last Anchor Master Record shall be set to the corresponding value in the Current Anchor Master Record, except that, if the NAN Device has become an Anchor Master due to starting a new NAN Cluster, the AMBTT in the Last Anchor Master Record shall be set to 0x00000000
- The AMR in the Current Anchor Master Record shall be set to its own Master Rank
- The Hop Count to Anchor Master in the Current Anchor Master Record shall be set to zero
- The AMBTT in the Current Anchor Master Record shall be set to 0x00000000

When a NAN Device starts a new NAN Cluster, it becomes the Anchor Master of the NAN Cluster.

A NAN Device that receives a NAN Synchronization Beacon frame with the Hop Count to Anchor Master value equal to zero shall use the lower four (4) octets of TSF from that frame as the AMBTT value in the NAN Cluster attribute.

A NAN Device shall discard a received NAN Synchronization Beacon frame if:

- The AMR value in the NAN Synchronization Beacon frame is equal to the corresponding value in the Current Anchor Master Record; and
- The AMBTT value in the NAN Synchronization Beacon frame is more than 16*512 TUs lower than the NAN Device's current TSF

NAN Synchronization Beacon frames that are not discarded shall be processed as specified in this specification to determine the Anchor Master of the NAN Cluster.

3. Anchor Master Record rules for determining which NAN Device becomes the Anchor Master

Upon receiving a NAN Synchronization Beacon frame that is not discarded, a NAN Device that is not an Anchor Master compares the AMR value in the Current Anchor Master Record with the corresponding value in the received frame.

1. If the AMR value in the Current Anchor Master Record is lower than that in the received frame, the NAN Device shall compare the AMR and AMBTT values in the Last Anchor Master Record with the corresponding values in the received frame and apply the following rules:
    a. If the AMR value in the received frame is equal to the corresponding value in the Last Anchor Master Record, and the AMBTT value in the received frame is less than or equal to the corresponding value in the Last Anchor Master Record, the NAN Device disregards the Anchor Master information in the received frame.

b. Otherwise, the NAN Device shall first update the AMR and the AMBTT values in the Last Anchor Master Record with the corresponding values in the Current Anchor Master Record. Subsequently, the NAN device shall update the Current Anchor Master Record as follows:
- The AMR value shall be set to the corresponding value in the received frame

- The Hop Count to Anchor Master value shall be set to the corresponding value in the received frame plus one

- The AMBTT shall be set to the corresponding value in the received frame

2. If the AMR value in the Current Anchor Master Record is higher than that in the received frame, the NAN Device shall further compare the lower 6-octet of the AMR value in the Current Anchor Master Record with the lower 6-octet of the AMR value in the received frame and apply the following rules:

   a. If the lower 6-octet of the AMR value in the Current Anchor Master Record is not equal to that in the received frame, the NAN Device shall disregard the Anchor Master information in the received frame.

   b. If the lower 6-octet of the AMR value in the Current Anchor Master Record is equal to that in the received frame, the NAN Device shall compare the AMR value in the received frame with the NAN Device's own Master Rank value and apply the following rules:

      If the AMR value in the received frame is lower than the NAN Device's own Master Rank value, the NAN Device shall assume itself as an Anchor Master and update its Last Anchor Master Record and its Current Anchor Master Record accordingly

      If the AMR value in the received frame is higher than the NAN Device's own Master Rank value, the NAN Device shall first update the AMR and the AMBTT values in the Last Anchor Master Record with the corresponding values in the Current Anchor Master Record. Subsequently, the NAN device shall update the Current Anchor Master Record as follows:

      - The AMR shall be set to the corresponding value in the received frame

      - The Hop Count to Anchor Master value shall be set to the corresponding value in the received frame plus one

      - The AMBTT shall be set to the corresponding value in the received frame

      NOTE: The lower 6-octets of the AMR value are derived from the corresponding Anchor Master's NAN Interface Address. When comparing the lower 6-octet of the Anchor Master in the Current Anchor Master Record with that in the Beacon frame, a NAN Device may tell whether the recorded Anchor Master is the same as the Anchor Master that originates the Anchor Master information in the received frame.

3. If the AMR value in the Current Anchor Master Record is equal to that in the received frame, the NAN Device shall compare the AMBTT value in the Current Anchor Master Record with that in the received frame and compare the Hop Count to Anchor Master value in Current Anchor Master Record with the corresponding value in the received frame and apply the following rules:

   a. If the AMBTT value in the Current Anchor Master Record is smaller than that in the received frame, the NAN Device shall adopt the AMBTT value in the received frame as the corresponding value in the Current Anchor Master Record; otherwise, the NAN Device disregards the AMBTT information in the received frame.

   b. If the Hop Count to Anchor Master value in the Current Anchor Master Record is larger than the corresponding value in the received frame plus one, the NAN Device shall adopt the Hop Count to Anchor Master value in the received frame plus one as the corresponding value in the Current Anchor Master Record; otherwise, the NAN Device disregards the Hop Count to Anchor Master information in the received frame.

Upon receiving a NAN Synchronization Beacon frame that is not discarded, a NAN Device that is an Anchor Master shall disregard the Anchor Master information in the received frame if the AMR value in the received frame is lower than the NAN Device's Master Rank value, or if the lower 6-octet of the AMR value in the received frame is equal to the lower 6-octet of the NAN Device's Master Rank value; otherwise, the NAN Device shall first update the AMR and the AMBTT values in the Last Anchor Master Record with the corresponding values in the Current Anchor Master Record. Subsequently, the NAN device shall update the Current Anchor Master Record as follows:

- The AMR shall be set to the corresponding value in the received frame
- The Hop Count to Anchor Master field value shall be set to the corresponding value in the received frame plus one
- The AMBTT shall be set to the corresponding value in the received frame

If a NAN Device needs to update its Current Anchor Master Record based on a received NAN Synchronization Beacon frame, it shall update the record before performing master election and state transition as specified in section 3.3.5.

NOTE: The 4-octet AMBTT value wraps over approximately every 71 minutes. Implementations are advised to resolve any ambiguity that may occur.

4. Anchor Master Record Expiration

If a NAN Device that is not an Anchor Master has not updated AMBTT in its Current Anchor Master Record for three (3) contiguous participated DWs, it shall assume itself as an Anchor Master and update its Last Anchor Master Record and its Current Anchor Master Record accordingly.

If a NAN Device that is not an Anchor Master has not received any NAN Synchronization Beacon frames with the Hop Count to Anchor Master value less than the corresponding value in the Current Anchor Master Record for three (3) contiguous participated DWs, while the AMBTT value in its Current Anchor Master Record has been updated at least once during those three (3) DWs, it shall set the Hop Count to Anchor Master value in the Current Anchor Master Record to 255.

5. NAN Device Updating its Own Master Rank

Upon changing any of the Master Rank components (Master Preference, Random Factor, NAN Interface Address) a NAN Device that is not an Anchor Master shall compare the resulting new Master Rank value with the AMR value in the Current Anchor Master Record. If the NAN Device's new Master Rank is higher than the AMR value in its Current Anchor Master Record, it shall assume itself as an Anchor Master and update its Last Anchor Master Record and its Current Anchor Master Record accordingly.

Upon changing any of the Master Rank components (Master Preference, Random Factor, NAN Interface Address), a NAN Device that is an Anchor Master shall continue serving as an Anchor Master and update its Last Anchor Master Record and its Current Anchor Master Record accordingly.

3.3.4.2 Anchor Master Information in NAN Beacon frames

A NAN Device shall set the Anchor Master field of the Cluster attribute in the NAN Synchronization and NAN Discovery Beacon frames that it transmits to the corresponding values in its Current Anchor Master Record.

A NAN Device that transmits a NAN Synchronization Beacon or NAN Discovery Beacon frame shall ensure that the TSF of that frame is derived from the same Anchor Master that is contained in the Cluster attribute.

3.3.5 Adjusting the TSF Timer

A NAN Device that is not an Anchor Master shall adopt the TSF timer value in a NAN Synchronization Beacon frame received with the same Cluster ID as the NAN Device's own Cluster ID, and may adopt the TSF timer value in a NAN Discovery Beacon frame received with the same Cluster ID as the NAN Device's own Cluster ID, when the AMR value in the received frame is:

- Higher than the corresponding value in the NAN Device's Current Anchor Master Record, and is different from the corresponding value in the Last Anchor Master Record, or
- Higher than the corresponding value in the NAN Device's Current Anchor Master Record and is equal to the corresponding value in the Last Anchor Master Record, and the AMBTT value in the received frame is larger than the corresponding value in the Last Anchor Master Record, or
- Lower than the corresponding value in the NAN Device's Current Anchor Master Record, but higher than the NAN Device's own Master Rank value, and the lower 6-octets of the AMR value in the received frame is equal to that in the NAN Device's Current Anchor Master Record, or
- Equal to the corresponding value in the NAN Device's Current Anchor Master Record, and the AMBTT value in the received frame is larger than the corresponding value in the Current Anchor Master Record

A NAN Device that is an Anchor Master shall adopt the TSF timer value in a NAN Synchronization Beacon frame received with the same Cluster ID as the NAN Device's own Cluster ID and may adopt the TSF timer value in a NAN Discovery Beacon frame received with the same Cluster ID as the NAN Device's own Cluster ID, when the AMR value in the received frame is higher than the NAN Device's Master Rank value and the lower 6-octet of the AMR value in the received frame is different from the lower 6-octet of the NAN Device's Master Rank value.

3.3.6 NAN Device Role and State Transition in the 2.4 GHz frequency band

A NAN Device shall assume the role of a Master when it starts or joins a NAN Cluster, and shall remain in the Master role unless it transitions to a NAN Non-Master role during a DW. A NAN Device in a NAN Non-Master role shall remain in the NAN Non-Master role, and only transitions to a NAN Master role at the end of a DW if such a transition occurs.

When a NAN Device switches from a Master role to a non-Master role, it shall initially assume a Sync state, until it transitions to a Non-Sync state during a DW, if such a transition occurs. A NAN Device in a Non-Master Non-Sync state shall remain in the Non-Sync state, and only transitions to a Non-Master Sync state or transitions to a Master role at the end of a DW, if such a transition occurs.

The NAN Device role and state transition is illustrated in Figure 11.

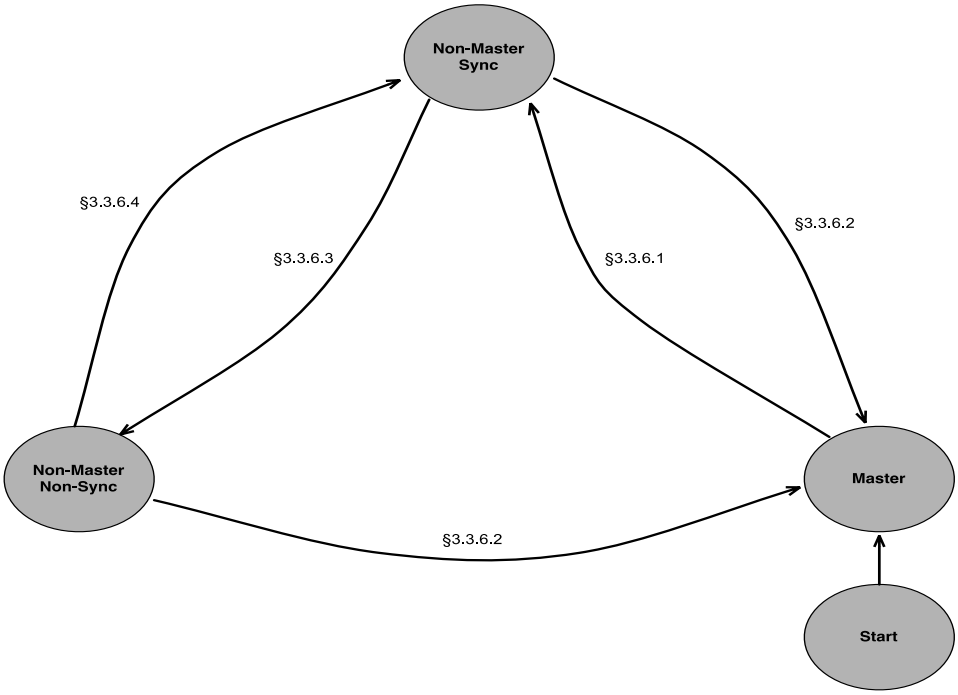


Figure 11. NAN Device Role and State Transition

To achieve stable and smooth NAN Device role and state transitions, a NAN Device should evaluate a moving average of the RSSI value of the transmitters' NAN Synchronization and NAN Discovery Beacon frames to make role and state transition decisions.

3.3.6.1 NAN Master to Non-Master Sync State Transition

During a DW, a NAN Device shall change its role and state from Master to Non-Master Sync if:

- It receives a NAN Synchronization Beacon frame with the RSSI[1] higher than RSSI_close from a NAN Device within the same NAN Cluster, and the Master Rank of the NAN Synchronization Beacon transmitter is higher than the device's Master Rank, or

[1] The RSSI value that should be used is the moving average RSSI value.

- It receives NAN Synchronization Beacon frames from three or more NAN Devices within the same NAN Cluster with RSSI[1] higher than RSSI_middle and the Master Rank of those devices are higher than the Master Rank of the receiving device

The value for RSSI_close shall be greater than -60 dBm. The value for RSSI_middle shall be greater than -75 dBm and less than the value defined for RSSI_close.

During a DW, if a NAN Device in a Master role receives a Beacon or a set of Beacon frames that fulfill the rules in both section 3.3.6.1 and 3.3.6.3, it transits its role and state to Non-Master Sync state, and then transits to Non-Master Non-Sync state.

3.3.6.2 NAN Non-Master to Master Role Transition

At the end of a DW, a NAN Device shall change its role from Non-Master to Master if during the DW:

- It does not receive any NAN Synchronization Beacon frames with the RSSI[1] higher than RSSI_close from a NAN Device within the same NAN Cluster, and the Master Rank of the NAN Synchronization Beacon transmitter is higher than the device's Master Rank, and
- It receives NAN Synchronization Beacon frames from less than three NAN Devices within the same NAN Cluster with RSSI[1] higher than RSSI_middle and the Master Rank of those devices are higher than the Master Rank of the receiving device

3.3.6.3 NAN Non-Master Sync to Non-Master Non-Sync State Transition

During a DW, a NAN Device in a Non-Master role shall change its state from Sync to Non-Sync if either of the following two conditions is met:

- It receives a NAN Synchronization Beacon frame with the RSSI[1] higher than RSSI_close from a NAN Device within the same NAN Cluster, and
  - AMR value of the NAN Synchronization Beacon frame is equal to the NAN Device's recorded AMR value, and

    Hop Count field value of the NAN Synchronization Beacon frame transmitter is lower than the NAN Device's Hop Count field value, or

    Hop Count field value is equal to the NAN Device's Hop Count, and the Master Rank of the NAN Synchronization Beacon frame transmitter is higher than the NAN Device's Master Rank
- It receives NAN Synchronization Beacon frames from three or more NAN Devices within the same NAN Cluster with RSSI[1] higher than RSSI_middle, and
  - AMR value of those devices' NAN Synchronization Beacon frame is equal to the NAN Device's recorded AMR value, and
  - Hop Count field value of the NAN Synchronization Beacon frame transmitter is lower than the NAN Device's Hop Count field value, or
  - Hop Count field value is equal to the NAN Device's Hop Count, and the Master Rank of the NAN Synchronization Beacon frame transmitter is higher than the NAN Device's Master Rank

3.3.6.4 NAN Non-Master Non-Sync to Non-Master Sync State Transition

At the end of a DW, a NAN Device in a Non-Master role shall change its state from Non-Sync to Sync if both following conditions are met:

- It does not receive any NAN Synchronization Beacon frames with the RSSI[1] higher than RSSI_close from a NAN Device within the same NAN Cluster, and
  - AMR value of the NAN Synchronization Beacon frame is equal to the NAN Device's recorded AMR value, and
  - Hop Count field value of the NAN Synchronization Beacon frame transmitter is lower than the NAN Device's Hop Count field value, or
  - Hop Count field value is equal to the NAN Device's Hop Count, and the Master Rank of the NAN Synchronization Beacon frame transmitter is higher than the NAN Device's Master Rank

- It receives NAN Synchronization Beacon frames from less than three NAN Devices within the same NAN Cluster with RSSI[1] higher than RSSI_middle, and
  - AMR value of those devices' NAN Synchronization Beacon frame is equal to the NAN Device's recorded AMR value, and
  - Hop Count field value of the NAN Synchronization Beacon frame transmitter is lower than the NAN Device's Hop Count field value, or
  - Hop Count field value is equal to the NAN Device's Hop Count, and the Master Rank of the NAN Synchronization Beacon frame transmitter is higher than the NAN Device's Master Rank

At the end of a DW, a NAN Device in a Non-Master Non-Sync state shall change its role from Non-Master to Master if conditions in section 3.3.6.2 are met otherwise it shall change its state to Non-Master Sync if the conditions in section 3.3.6.4 are met.

3.3.6.5 NAN Beacon Transmission and Suppression

If a NAN Device has a Master role or has a Non-Master role Sync state at the start of a DW, it shall initiate a NAN Synchronization Beacon frame transmission by starting the DW Contention Mitigation procedure defined in section 3.5.1 at the beginning of the DW.

If the NAN Device assumed itself as an Anchor Master (as defined in section 3.3.4.1) from a Non-Master role non-Sync state in the previous DW, it should cancel its NAN Synchronization Beacon frame transmission within the DW.

During the DW, if a NAN Device changes its role and state to Non-Master Non-Sync before its back-off counter has a value of zero, it shall cancel its NAN Synchronization Beacon frame transmission within the DW; otherwise, it shall transmit a NAN Synchronization Beacon frame according to the DW Contention Mitigation procedure in section 3.5.1.

A NAN Device shall not transmit more than one NAN Synchronization Beacon frame within a DW.

If a NAN Device has a Non-Master role Non-Sync state at the start of a DW, it shall not initiate a NAN Synchronization Beacon frame transmission during the DW.

If a NAN Device changes its role from Non-Master to Master at the end of a DW, it shall not transmit any NAN Discovery Beacon frames regularly before the next DW, but with the following exceptions:

- It is allowed to skip transmission of a NAN Discovery Beacon if the intended transmission time overlaps with a NAN DW of the NAN Cluster where the NAN Device is participating in; or
- It is allowed to skip transmission of a NAN Discovery Beacon if the intended transmission time overlaps with its committed availability period for one of its NDP(s) on a channel different from channel 6 and 149 or 44
- It is allowed to skip transmission of a NAN Discovery Beacon if the intended transmission time overlaps ranging Committed Ranging Schedules (CRSs) on a channel different from channel 6 and 149 or 44

If a NAN Device is in Non-Master role (either in Sync state or Non-Sync state) at the end of a DW, it should not transmit NAN Discovery Beacon frames regularly. Note that a NAN Device in Non-Master role may transmit NAN Discovery Beacon frames reactively for a short period to expedite the NAN cluster and service discovery in its neighborhood.

3.3.7 NAN Device role and state transition in the 2.4 GHz and 5 GHz frequency band

If a NAN Device operates in the 5 GHz frequency band,

- It should recommence NAN Synchronization Beacon frame transmission at the beginning of each 5 GHz DW, according to the DW Contention Mitigation procedure in section 3.5.1, only if it is in a Master role or is in the Non-Master Sync state during the entire 2.4 GHz DW immediately before the 5 GHz DW
- It should perform NAN Device role and state transitions as specified in section 3.3.6 as if the 5 GHz DW and the immediately preceding 2.4 GHz DW are a contiguous single DW

Table 6 lists the NAN Device role and state transitions in 2.4 GHz and 5 GHz DWs.

Table 6. NAN Device role and state transition in DWs

2.4 GHz DW	5 GHz DW (128 TUs after the 2.4 GHz DW)	Role and state transition
Committed	Committed	Start from the beginning of the 2.4 GHz DW May continue in 5 GHz DW Complete at the end of 2.4 GHz DW or 5 GHz DW
Committed	Non-committed	Start from the beginning of the 2.4 GHz DW Complete at the end of the 2.4 GHz DW
Non-committed	Committed	May start from the beginning of the 5 GHz DW and complete at the end of the 5 GHz DW
Non-committed	Non-committed	No Role / State Transition

The RSSI thresholds used for NAN Master Selection and Non-Master state transition in the 5 GHz DW shall be RSSI_50_close, and RSSI_50_middle, respectively. The value of RSSI_50_close shall be greater than -60 dBm. The value for RSSI_50_middle shall be greater than -75 dBm and less than the value defined for RSSI_50_close.

If a NAN Device maintains the Master role at the end of the combined 2.4 GHz and 5 GHz DWs, it shall transmit NAN Discovery Beacon frames on the 2.4 GHz NAN Discovery Channel according to section 3.3.8.1 until the next DW. It may transmit NAN Discovery Beacon frames on the 5 GHz NAN Discovery Channel according to section 3.3.8.1 until the next DW.

If a NAN Device receives a NAN Synchronization Beacon frame during the 5 GHz DW, it should update its TSF timer as described in section 3.3.5.

NAN Devices that intend to transmit NAN Service Discovery frames during a 5 GHz DW shall mitigate contention during the DW according to the procedure specified in section 3.5.1 and 3.5.3. Such NAN Devices shall maintain separate Contention Window parameters and Transmission Window for both the 2.4 GHz DW and the 5 GHz DW.

3.3.8 NAN Discovery and acquiring synchronization

Discovery of NAN Clusters occurs through passive scanning in the NAN Discovery Channel in the 2.4 GHz and, if supported by the NAN Device, in the 5 GHz frequency bands. A passive scan performed by a NAN Device is implementation specific.

In addition, NAN clusters may also be discovered through Beacon or Probe Response frames that carry a Cluster Discovery attribute (section 9.5.2). Any Wi-Fi Device that transmits Beacon or Probe Response frames and are aware of one or more NAN Clusters should include the NAN IE with Cluster Discovery attributes for each NAN Cluster they are aware of.

If several NAN Clusters are discovered, a NAN Device shall select a NAN Cluster to join according to section 3.4.

3.3.8.1 NAN Discovery Beacon frame transmission

Each NAN Device in Master role shall transmit NAN Discovery Beacon frames outside NAN Discovery Windows to facilitate the discovery of the NAN Cluster. The following rules shall be used to transmit NAN Discovery Beacon frames:

- The time between consecutive NAN Discovery Beacon frames transmitted by the same NAN Device in Master role shall be smaller than 200 TUs
- The time between consecutive NAN Discovery Beacon frames transmitted by the same NAN Device in Master role shall be larger than 50 TUs

To minimize the power required to transmit NAN Discovery Beacon frames, a NAN Device in Master role shall use the default AC_VO contention settings defined in [4] for the transmission of NAN Discovery Beacon frames.

Figure 12 illustrates the transmission of NAN Discovery and NAN Synchronization Beacon frames when a NAN Device is operating in the 2.4 GHz frequency band.

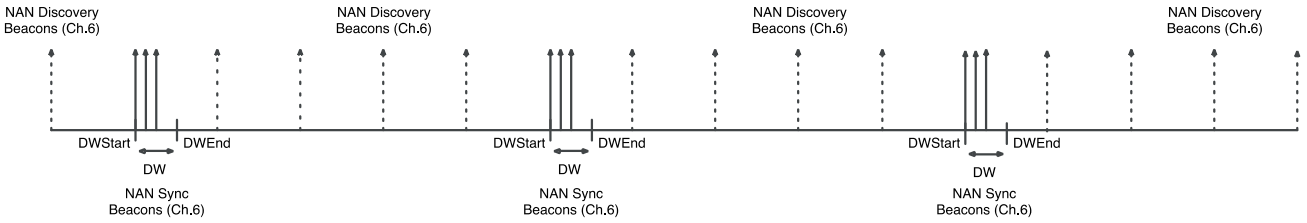


Figure 12. NAN Synchronization and NAN Discovery Beacon frame transmission on 2.4 GHz NAN Discovery Channel

Figure 13 illustrates an example of the transmission of NAN Discovery and NAN Synchronization Beacon frames when a NAN Device is operating in the 2.4 GHz and 5 GHz frequency bands with the same beacon intervals.

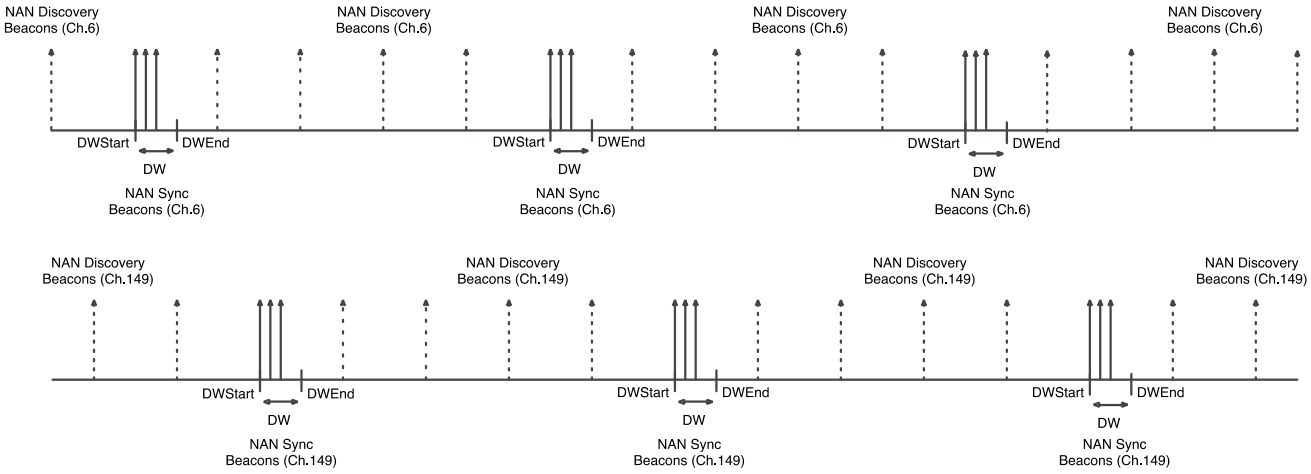


Figure 13. NAN Synchronization and NAN Discovery Beacon frame transmission on 2.4 GHz and 5 GHz NAN Discovery Channel

Recommended practices on the transmission of NAN Discovery Beacon frames can be found in Appendix B.

3.4 NAN Cluster selection and merging

3.4.1 NAN Cluster initiation and selection

Upon activating NAN functionality, a NAN Device shall perform passive scanning and may start a NAN Cluster.

If one or more NAN Clusters are discovered, the NAN Device shall join the cluster with highest cluster grade (CG).

If one or more NAN Clusters have the same highest CG, the NAN Device shall join the NAN Cluster with the highest AMR.

Upon joining a NAN Cluster, a NAN Device shall adopt the parameters of the NAN Cluster including the TSF value.

To join a NAN Cluster that a NAN Device has discovered through a Cluster Discovery attribute in a Probe Response frame, the NAN Device only needs to wake up at the Discovery Window times computed using the Time Offset field in the Cluster Discovery attribute to participate in the NAN Cluster.

3.4.1.1 NAN Cluster Grade

Each NAN Cluster shall have a Cluster Grade (CG) that is determined as follows:

CG = 2^64*A1+A2

Where A1 is the Master Preference of the Anchor Master of the NAN Cluster and A2 is the value of the 8-octet TSF value of the NAN Cluster with the lower 19 bits of the TSF value set to zero.

3.4.2 NAN Cluster merging

Two NAN Clusters merge as NAN Devices in one NAN Cluster discover the existence of another NAN Cluster and converge into a common NAN Cluster.

A NAN Device that operates in a NAN Cluster shall determine the CG of its own NAN Cluster, scan for other NAN Clusters and determine the CGs of the discovered NAN Clusters. When a NAN Device that operates in a NAN Cluster receives a NAN Synchronization Beacon frame or a NAN Discovery Beacon frame with a Cluster ID different from the recorded Cluster ID, it decides that there is more than one Cluster. If one or more NAN Clusters with higher CG than the CG of the NAN Device's current NAN Cluster are discovered, the NAN Device shall stop participating in the current NAN Cluster and join the NAN Cluster with the highest CG. If one or more NAN Clusters have the same highest CG, the NAN Device shall join the NAN Cluster with the highest AMR.

When a NAN Device decides to join a NAN Cluster with higher CG, and if the NAN Device assumes the role of Master or Non-Master Sync in the previous NAN Cluster, it should propagate the cluster merging by sending once in the DW of the previous NAN Cluster a NAN Synchronization Beacon frame with the NAN IE containing the information corresponding to the new cluster and with the A3 address field in the NAN Synchronization Beacon frame (see Figure 57) set to the new cluster ID. The transmission procedure used for such a Beacon frame shall follow the procedure for transmission of NAN Service Discovery frames given in section 3.5.

When joining a new NAN Cluster through cluster merging, a NAN Device shall assume the same role and state as it had in the previous NAN Cluster. During the first DW after joining the new NAN Cluster, if the NAN Device had a Master role or had a Non-Master role Sync state in the previous NAN Cluster, it shall initiate a NAN Synchronization Beacon frame transmission by starting the DW Contention Mitigation procedure defined in section 3.5.1 at the beginning of the first DW; if the NAN Device had a Non-Master role Non-Sync state in the previous NAN Cluster, the NAN Device shall not initiate a NAN Synchronization Beacon frame transmission during the first DW.

At the end of first DW, the NAN Device shall follow the procedures in section 3.3.6.5.

3.5 Operating in the Discovery Window

A NAN Device may transmit the following NAN management frames in a DW:

- NAN Synchronization Beacon frame
- NAN Service Discovery frame (SDF)
- NAN Action frame (NAF)

A NAN Device shall not transmit NAN data frames in a DW on the designated discovery channel. This section specifies mechanisms to manage transmission of frames by NAN Devices in a Discovery Window that limit the number of NAN Devices that contend during a DW and to minimize collisions by devices that contend during the DW are specified. Section 3.5.1 describes the contention scheme to minimize collisions and section 3.5.3 describes the protocol to limit the number of devices that contend during a DW.

A NAN Device may include one or more NAN attributes in a NAN SDF or a NAN NAF. In a DW, the duration of the PPDU that carries the NAN SDF or the NAN NAF should not exceed 200 microseconds but shall not exceed 400 microseconds.

3.5.1 Discovery Window contention mitigation

Two contention window parameters are required, and these are denoted by CW and CW_RS.

Notation:

- TStartDW: Denotes the start time of a DW
- TEndDW: Denotes the end time of a DW
- Tpkt(p): Time that a packet p is available for transmission in a DW, (TStartDW ≤ Tpkt(p) ≤ TEndDW)

If multiple NAN SDFs or NAFs were buffered for transmission prior to the start of a DW, Tpkt(p) of the first NAN SDF or NAF is set to TStartDW, and the Tpkt(p) of a subsequent NAN SDF or NAF is set to a time after the transmission completion time of the preceding NAN SDF or NAF.

For a NAN Synchronization Beacon frame, Tpkt(p) = TStartDW+mod(HC,10)*40*aSlotTime, where HC is the Hop Count to Anchor Master value in the recorded Anchor Master information determined at TStartDW, and aSlotTime is per the definition in [1].

For a NAN SDF or NAF (first transmission or retransmission), a back-off counter c_dw shall be set to a value randomly drawn from a uniform distribution over the interval [0, CW]. In addition, a time Trs(p) shall be set to a value randomly drawn from a uniform distribution over the interval [Tpkt(p), TEndDW]. If at Trs(p) the c_dw has a non-zero value, the c_dw shall be set to a value randomly drawn from a uniform distribution over the interval [0, CW_RS] if the randomly drawn value is less than the residual value in the c_dw. Whenever the c_dw reaches zero, either before or after Trs(p), the NAN SDF or NAF shall be transmitted.

For a NAN Synchronization Beacon frame, a back-off counter c_dwb shall be set to a value randomly drawn from a uniform distribution over the interval [0, CW_RS] when HC is equal to zero or [0, 31] when HC is greater than zero.

For the transmission of a NAN SDF, a NAF, or a NAN Synchronization Beacon frame, the back-off counter c_dw and c_dwb shall be decremented according to the back-off count down procedure given in section 10.3.4 of [1]. When the countdown reaches zero, the associated frame shall be transmitted.

When a NAN Device starts to count down a back-off counter for a NAN Synchronization Beacon frame transmission while the back-off counter for a NAN SDF or NAF has a non-zero value, it may suspend the countdown of the back-off counter for the NAN SDF, or NAF, and resume the countdown of that back-off counter after the NAN Synchronization Beacon frame is transmitted.

If the c_dw of a NAN SDF or NAF or the c_dwb of a NAN Synchronization Beacon frame does not count down to zero prior to TEndDW, the transmission of the associated frame is aborted. The sender may attempt to transmit the aborted frame in a subsequent DW using the procedure outlined above. If a NAN SDF or NAF was carried over from a previous DW due to the contention countdown not being completed, the c_dw may be set to the residual counter value left from the previous DW.

The AIFSN value for all NAN transmissions in a DW shall be set to two (2). Suggested values for CW and CW_RS are given in Table 7.

Table 7. Suggested CW and CW_RS values

Parameter	Value
CW	511
CW_RS	15

Within a DW, if a NAN Device determines the medium is not busy for the length of the CW, the NAN Device may assume there are no further NAN transmissions.

3.5.2 Multiple frame transmission from a NAN Device in a Discovery Window

A NAN Device shall not transmit more than one NAN Synchronization Beacon frame in a DW. Multiple NAN SDFs or NAFs may be transmitted by a NAN Device in a DW.

However, for channel efficiency, a NAN Device should avoid transmitting multiple NAN SDFs or NAFs within the same DW. If multiple Service Descriptors are available for transmission in a DW, the NAN Device should aggregate the Service Descriptor Attributes into a single NAN SDF.

3.5.3 Limiting the number of NAN Devices that contend during a Discovery Window

A Discovery Window is only able to accommodate a limited number of transmissions. To reduce the probability of collision when a large number of NAN Devices compete for access, a NAN Device that has a NAN SDF or NAF ready for transmission shall use the following procedure to limit transmissions to a subset of the Discovery Windows.

1. A NAN Device maintains a state variable TW (denoting Transmit Window) initialized to zero.

2. The NAN Device that has a new NAN SDF or NAF available for transmission chooses an integer number n from a uniform random distribution in the range [0 to TW].
3. The NAN Device begins channel access (as in section 3.5.1) to transmit the NAN SDF or NAF at the start of the nth DW, where n = 0 represents the DW with a start time greater than the current TSF timer value.
4. If the frame transmission begins before start time of nth DW + 0.75 * DW duration, then TW is set as follows: TW = max {0, (TW – 1)} and the corresponding n is chosen as in step 2 for the next NAN SDF or NAF transmission.
5. Otherwise, TW is set as follows: TW = min {16, (TW + 2)} and the corresponding n is chosen as in step 2 for the next NAN SDF or NAF transmission.

This procedure allows a NAN Device to transmit on average one NAN SDF or NAF every TW Discovery Windows. A NAN Device can include multiple Service Descriptor Attributes in each NAN SDF as described in section 9.5.4.

3.6 Operating outside the Discovery Window

When a NAN Device transmits frames outside DWs, it should use the default WMM EDCA parameters for Non-AP STA, as specified in Table 8.

Table 8. Default WMM parameters for a STA

AC	CWmin	CWmax	AIFSN	TXOP Limit (802.11a/g/n/ac)
AC_BK	15	1023	7	0
AC_BE	15	1023	3	0
AC_VI	7	15	2	94 (3.008 ms)
AC_VO	3	7	2	47 (1.504 ms)

4 NAN Service Discovery

NAN Service Discovery frames enable NAN Devices to look for services from other NAN Devices and make services discoverable for other NAN Devices. There are two NAN Service Discovery protocol messages defined in the NAN Service Discovery Protocol:

1. Publish message
2. Subscribe message

The NAN Service Discovery protocol messages shall be carried in Service Descriptor Attributes that are carried in the NAN Service Discovery frames.

A NAN Device may use a NAN Service Discovery frame to actively search for availability of a specific service. When a NAN Device sends a Subscribe message, it asks for other NAN Devices operating in the same NAN Cluster to transmit a Publish message it the response criteria are met.

A NAN Device may use a Publish message to make its service(s) discoverable for other NAN Devices operating in the same NAN Cluster in an unsolicited manner.

4.1 NAN Discovery Engine

This section outlines the procedures for the operations of the NAN Discovery Engine.

Figure 14 illustrates a NAN Discovery Engine and its internal components and interfaces, as well as a possible architecture for the NAN Discovery Engine.

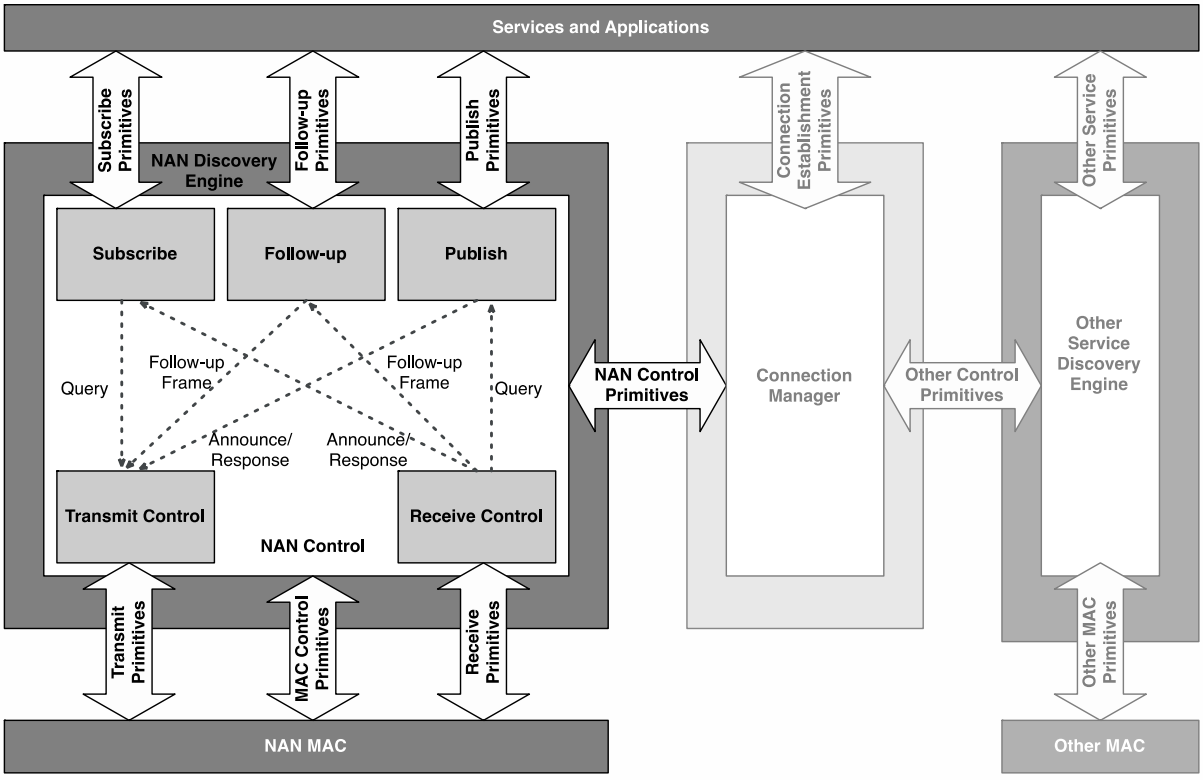


Figure 14. Logical reference architecture for NAN Discovery Engine

The Subscribe, Publish, and Follow-up primitives cover the NAN Discovery functionality. Services and applications using the NAN Discovery Engine should have no need to know the details of the NAN Discovery Engine operation, nor should they have a need to know about possible further connection establishment parameters. NAN MAC specific functionality,

for example if and when to include a Service ID Attribute in a NAN Synchronization Beacon frame, is implementation specific and is outside the scope of the NAN Service Interface.

NAN Control primitives may carry information tangential to the NAN Discovery functionality, such as the information that may be carried in the optional NAN Connection Capability, WLAN Infrastructure, Extended WLAN Infrastructure, P2P Operation, and Extended P2P Operation Attributes. This information may be helpful in post-NAN Discovery operations. However, the exact format and use of these NAN Control primitives are implementation specific and are outside the scope of this specification.

4.1.1 Service interface

The NAN Discovery Engine is accessible to services in the NAN Device through a logical interface that is described in terms of Method and Event primitives.

A Method represents actions initiated by a service/application, with information about the action to be taken contained in the Method parameters. Limited information is returned to the caller in a Method call return value. All Method calls shall return immediately, so their return value cannot depend on information obtained over the air.

Events provide information from the NAN Discovery Engine to the services/applications. Like Methods, Events carry data in parameters.

Multiple services/applications in communication with the NAN Discovery Engine uses Methods and Events. Methods propagate from a service/application to the NAN Discovery Engine. Events propagate from the NAN Discovery Engine to a specific service/application. Events are not necessarily in direct response to a Method call.

4.1.1.1 Methods

Publish

Publish(service_name, matching_filter_tx, matching_filter_rx, service_specific_info, configuration_parameters, datapath_parameters, qos_requirements, range_configuration_parameters, security_configuration_parameters, pairing_configuration_parameters, USD_configuration_parameters)

With this Method a service/application makes a service discoverable with given parameters for other NAN Devices by publishing it.

Parameters of the Method Publish are as follows:

- service_name
  - UTF-8 name string which identifies the service/application
- matching_filter_tx
  - Ordered sequence of <length, value> pairs to be included in the discovery frame
- matching_filter_rx
  - Ordered sequence of <length, value> pairs that specify further the response conditions beyond the service name used to filter the subscribe messages
- service_specific_info
  - Sequence of values that are conveyed in the Publish message.
- configuration_parameters
  - Publish type

    Determines the type of Publishing as follows

    - Unsolicited transmissions only

    - Solicited transmissions only

    - Both unsolicited and solicited transmissions

- Discovery range

  - Determines whether the service is made discoverable to only NAN Devices in close proximity only or to any NAN Devices within range

- Solicited transmission type

  - Determines whether a solicited transmission is a unicast or a multicast transmission

- Announcement period

  - Recommended periodicity of unsolicited transmissions

- Time to live

  - The instance of the Publish function can be commanded to run for a given time interval or for one transmission only

- Event conditions

  - Determines when Publish related events are generated. Event requests may be generated on each solicited transmission or not at all.

- Matching filter flag

  - Zero if matching_filter_tx is equal to matching_filter_rx

  - One if matching_filter_tx is not equal to matching_filter_rx

- NAN Ranging flag

  - Zero if NAN Ranging is optional for the service discovery

  - One if NAN Ranging is mandatory for the service discovery

- Data Path flag

  - Zero if NDP setup is not required for the service

  - One if NDP setup is required for the service

- Awake DW Interval

  - The interval in units of 512 TUs between two DWs in during which the device supporting the service is awake to transmit or receive corresponding the Service Discovery frames.

  - Valid values are: 1, 2, 4, 8 and 16.

- Further Service Discovery flag

  - Zero if Further Service Discovery is not required

  - One if Further Service Discovery is required

- Further Service Discovery function

  - An optional parameter that is only present when the Further Service Discovery flag is set to one:

  Zero if Follow-up is used;

  One if GAS is used

- NAN Discovery flag

  -Zero if NAN Synchronization used for Device/Service Discovery

  -One if USD used for Device/Service Discovery

- datapath_parameters (Optional, and present only if the Data Path flag is set to 1)

  - Data Path Type

- Zero if NDP setup is required for unicast
- Other values are reserved

  - QoS
    - Zero indicates QoS requirements are not present
    - One indicates QoS requirements are present
  - Security
    - Zero indicates open security
    - One indicates security required

- qos_requirements (Optional, and present only if the Data Path Type is set to 0 and the QoS is set to 1)
  - Unicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packets for MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- qos_requirements (Optional, and present only if the Data Path Type is set to 1 and the QoS is set to 1)
  - Multicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packets for MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- range_configuration_parameters (optional)
  - Optional parameters that are present if the NAN Ranging flag is set to one; refer to section 8.2.1 for the definitions.
- security_configuration_parameters
  - Identifies if security is required
    - One or more Cipher Suite IDs
    - One or more PMKIDs for NCS-SK cipher suites
  - Identifies additional frame protection required
    - Group addressed data frame protection
    - Group addressed management frame protection
- pairing_configuration_parameters
  - Pairing setup
    - Zero if the pairing setup is disabled
    - One if the pairing setup is enabled
  - NPK/NIK caching
    - Zero if the NPK/NIK caching is disabled

- One if the NPK/NIK caching is enabled

- Pairing verification
  - Zero if the pairing verification is disabled
  - One if the pairing verification is enabled
- Pairing bootstrapping
  - Supported bootstrapping methods
  - Comeback delay, if comeback is required

- USD_configuration_parameters (Optional, and parameters are relevant when the NAN Discovery flag is set to one)
  - defaultPublishChannel: indicates the defaultPublishChannel used in the USD
  - publishChannelList: indicates the publishChannelList used in the USD
  - N_{min}: indicates minimum value of N used in the USD
  - N_{max}: indicates maximum value of N used in the USD
  - M_{min}: indicates minimum value of Mused in the USD
  - M_{max}: indicates maximum value of M used in the USD

Any NAN Device that solicits a Publish response SDF shall correctly receive and process both unicast and multicast frames.

The Method returns a non-zero publish_id that is assigned by the NAN Discovery Engine and which uniquely identifies the instance of the Publish function on this device.

CancelPublish

CancelPublish(publish_id)

With this Method a service/application requests cancellation of an instance of the Publish function.

Parameters of the Method CancelPublish are as follows:

- publish_id
  - The ID originally returned by an instance of the Publish function.

Subscribe

Subscribe(service_name, matching_filter_rx, matching_filter_tx, service_specific_info, configuration_parameters, range_configuration_parameters, security_configuration_parameters, pairing_configuration_parameters, USD_configuration_parameters)

With this Method a service/application requests that the NAN Discovery Engine to search for a service based on parameters given from other NAN Devices.

Parameters of the Method Subscribe are as follows:

- service_name
  - UTF-8 name string which identifies the service/application
- matching_filter_rx
  - Ordered sequence of <length, value> pairs used to filter out received publish discovery messages containing the service name
- matching_filter_tx
  - Ordered sequence of <length,value> pairs of active subscriptions included in the Discovery frame
- service_specific_info

  - Sequence of values which further specify the published service beyond the service name
- configuration_parameters
  - Subscribe type

    - Determines the type of Subscribe as follows

    Passive

    Active
  - Discovery range

    - Determines whether subscription services are searched only for NAN Devices in close proximity or in any NAN Devices within range
  - Query period

    - Recommended periodicity of query transmissions
  - Time to live

    - The instance of the Subscribe function can be commanded to run for a given time interval or until the first DiscoveryResult event
  - Matching filter flag

    - Zero if matching_filter_tx is equal to matching_filter_rx

    - One if matching_filter_tx is not equal to matching_filter_rx
  - NAN Ranging flag

    - Zero if NAN Ranging is Optional for the service discovery

    - One if NAN Ranging is Mandatory for the service discovery
  - Awake DW Interval

    - Interval in units of 512 TUs between two DWs during which the device supporting the service is awake to transmit or receive.

    - Valid values are: 1, 2, 4, 8 and 16.
  - NAN Discovery flag

    -Zero if NAN Synchronization used for Device/Service Discovery

    -One if USD used for Device/Service Discovery
- range_configuration_parameters (optional)
  - Optional parameters that are present when the NAN Ranging flag is set to one; refer to section 8.2.1.1 for the definitions
- security_configuration_parameters
  - Identifies if security is required

    - One or more Cipher Suite IDs

    - One or more PMKIDs for NCS-SK cipher suites
  - Identifies additional frame protection required

    - Group addressed data frame protection

    - Group addressed management frame protection
- pairing_configuration_parameters

  - Pairing setup
    - Zero if the pairing setup is disabled
    - One if the pairing setup is enabled
  - NPK/NIK caching
    - Zero if the NPK/NIK caching is disabled
    - One if the NPK/NIK caching is enabled
  - Pairing verification
    - Zero if the pairing verification is disabled
    - One if the pairing verification is enabled
  - Pairing bootstrapping
    - Supported bootstrapping methods
    - Comeback delay, if comeback is required
- USD_configuration_parameters (Optional, and parameters are relevant when the NAN Discovery flag is set to one)
  - defaultPublishChannel: indicates the defaultPublishChannel used in the USD
  - publishChannelList: indicates the publishChannelList used in the USD

The Method Subscribe returns a non-zero subscribe_id that is assigned by the NAN Discovery Engine and which uniquely identifies the instance of the Subscribe function on this device.

CancelSubscribe

CancelSubscribe(subscribe_id)

With this Method a service/application may request cancellation of an instance of the Subscribe function.

Parameters of the method are as follows:

- subscribe_id
  - As originally returned by the instance of the Subscribe function

Transmit

Transmit(handle, service_specific_info, configuration_parameters)

With this Method a service/application may request the NAN Discovery Engine to transmit a follow-up message with a given content to a given NAN Device and targeted to a given instance of the Publish function or the Subscribe function in the given NAN Device.

Parameters of the Method Transmit are as follows:

- handle
  - A valid publish_id or subscribe_id which has been originally returned by an instance of the Publish function or the Subscribe function respectively
- service_specific_info
  - Sequence of values which are to be transmitted in the frame body
- configuration_parameters
  - NAN Interface Address
    - MAC address of the NAN Device to which the frame will be sent

- Requestor Instance ID

  - Identifier of the Publish or Subscribe function instance for the NAN Device which will be sent the follow-up message

- Priority

  - Requested relative priority of the transmissions

- Bootstrapping Parameters (optional)

  - Type: request or response

  - Status: accepted or rejected, if type = response

  - Bootstrapping Method: requested or confirmed bootstrapping method

UpdatePublish

UpdatePublish(publish_id, service_specific_info)

With this Method, a service/application requests the NAN Discovery Engine to indicate that the service specific information corresponding to the instance of the Publish function has changed. The updated service specific information may be conveyed using Publish messages and/or FSD messages.

Parameters of the Method UpdatePublish are as follows:

- publish_id
  - Identifier that was returned by the Publish function instance.
- service_specific_info
  - Sequence of values that should be conveyed to the Discovery Engine of a NAN Device that has invoked a Subscribe method corresponding to this Publish method. The new value will override any service specific information previously passed to the Publish or UpdatePublish methods for this instance of the Publish function.

GASScheduleRequest

GASScheduleRequest(publish_id, address)

With this Method a service/application may request a schedule for GAS frames exchange.

Parameters of the Method GASScheduleRequest are as follows:

- publish Id
  - Identifier for the Publisher function instance associated with the further service discovery
- Address
  - NAN Management Interface Address of the peer NAN Device

4.1.1.2 Events

DiscoveryResult

DiscoveryResult(subscribe_id, service_specific_info, service_update_indicator, publish_id, address, range_measurement, FSD_parameters, datapath_parameters, qos_requirements, security_parameters, pairing_parameters)

When an instance of the Subscribe function exists, a DiscoveryResult event is sent for each published service that is found on any remote NAN Device that matches the conditions of the instance based on a received publish message. Multiple DiscoveryResult events on the same discovery result may be avoided by implementing redundancy detection in a NAN Discovery Engine. Redundancy detection mechanisms are implementation specific and are therefore not described in this specification.

Parameters of the Event DiscoveryResult are as follows:

- subscribe_id
  - Identifier that was originally returned by the instance of the Subscribe function
- service_specific_info
  - Sequence of values that were decoded from a frame received from the Publisher
- service_update_indicator (Optional, and present only if the service_update_indicator field is present in the Service Descriptor Extension attribute (refer to section 9.5.4.2) of the received Publish message)
  - Version of the service specific information corresponding to the Publish instance, which may be conveyed by Publish messages and/or FSD messages.
- publish_id
  - Identifier for the instance of the published service on a remote NAN Device
- address
  - NAN Interface Address of the Publisher
- range_measurement (optional)
  - Range measurement result. This parameter is present if both the publisher and subscriber support the ranging capability and invoked ranging in the Publish and Subscribe functions
- FSD_parameters (Optional, and present only if the FSD Required flag is set in the SDEA of the received publish message)
  - Zero if Follow-up is used
  - One if GAS is used
- datapath_parameters (Optional, and present only if the Data Path Required flag is set in the SDEA of the received publish message)
  - Data Path Type

    - Zero if NDP setup is required

    - Other values are reserved
  - QoS

    - Zero indicates QoS is NOT required

    - One indicates QoS is required
  - Security

    - Zero indicates open security

    - One indicates security required
- security_parameters
  - One or more Cipher Suite IDs
  - One or more PMKIDs for NCS-SK cipher suites
- pairing_parameters
  - Pairing setup

    - Zero if the pairing setup is disabled

    - One if the pairing setup is enabled
  - NPK/NIK caching

    - Zero if the NPK/NIK caching is disabled

    - One if the NPK/NIK caching is enabled

- Pairing verification
  - Zero if the pairing verification is disabled
  - One if the pairing verification is enabled
- Pairing bootstrapping
  - Supported bootstrapping methods
- Pairing relationship
  - Status: not paired or already paired
- - Paired peer handle, if already paired

Replied

Replied(publish_id, address, subscribe_id, range_measurement, service_specific_info)

When an instance of the Publish function is active and configured to generate Replied events, a Replied event is sent for each solicited transmission.

Parameters of the Event Replied are as follows:

- publish_id
  - The Identifier originally returned by the Publish function instance
- address
  - NAN Interface Address of the Subscriber that triggered the transmission of the Publish message
- subscribe_id
  - subscribe_id obtained from the Subscribe message
- range_measurement (optional)
  - Range measurement result. This parameter is present if both the publisher and subscriber support the ranging capability and invoked ranging in the Publish and Subscribe functions
- service_specific_info
  - Sequence of values which were decoded from a frame received from the Subscriber

PublishTerminated

PublishTerminated(publish_id, reason)

An instance of the Publish function has stopped and will not be generating any more Published message.

Parameters of the Event PublishTerminated are as follows:

- publish_id
  - The Identifier originally returned by the Publish function instance
- reason
  - Timeout, user request or Failure

SubscribeTerminated

SubscribeTerminated(subscribe_id, reason)

An instance of the Subscribe function has stopped and will not be generating any more DiscoveryResult Events.

Parameters of the Event SubscribeTerminated are as follows:

- subscribe_id

    - The Identifier originally returned by the Subscribe function instance
- reason
    - Timeout, user request or Failure

Receive

Receive(id, peer_instance_id, service_specific_info, address, range_measurement, bootstrapping_info)

A Receive event is sent

- On each follow-up message that is received with a Service ID for which an instance of the Publish function or the Subscribe function exists; or
- On ranging report message that is received while an instance of the Publish function requiring ranging as part of service discovery is active

Parameters of the Event Receive are as follows:

- id
    - The original publish_id or subscribe_id returned by Publish or the Subscribe function instance respectively.
- peer_instance_id
    - Identifier of the Publish function or the Subscribe function in the NAN Device from which this follow-up message was received. It may not be present for ranging report
- service_specific_info
    - Sequence of values that were decoded from the received frame
- address
    - NAN Interface Address of the NAN Device from which the frame was received
- range_measurement (optional)
    - Range measurement result. It is an optional field. It may be present if both publisher and subscriber support ranging capability and an instance of the Publish function requiring ranging as part of service discovery is active.
- bootstrapping_info (optional)
    - type: indication or confirm
    - status: accept or reject, if type = confirm
    - bootstrapping method: requested or confirmed bootstrapping method

GASScheduleConfirm

GASScheduleConfirm(status, publish_id, address)

Parameters of the Event GASScheduleConfirm are as follows:

- status
    - Decision (Accepted / Rejected)
    - Reason Code
- publish id
    - Identifier for the Publisher function instance associated with the further service discovery
- address
    - NAN Management Interface Address of the peer NAN Device

4.1.2 Configuration interface

The NAN Discovery Engine provides a logical interface to configure the NAN stack.

4.1.3 Publish function

The Publish function operates as per Publish commands from services/applications through the Service Interface. When the Publish command is executed, it generates an instance of the Publish function which may run for a given time interval or until one announcement or response is transmitted, whichever occurs first. Each instance of the Publish function has a publish_id that uniquely identifies the instance locally. The publish_id is also used across devices in NAN discovery to uniquely identify an instance of service on a specific device. Each instance of the Publish function runs independently and the number of concurrently supported instances of the Publish function is implementation dependent. The following description applies to each instance of the Publish function separately.

Each instance of the Publish function generates a Publish message per the following rules:

- The Hash Value field is set to indicate the output of the hash algorithm as defined in [3] with the service name from the Publish command as the input
- The service_specific_info from the Publish command are put into either the Service Info field of the SDA or the Service Info field of the SDEA. (Note that, due to the size limit of the Service Info field of the SDA, if the service_specific_info is longer than 255 bytes, the Service Info field of the SDEA should be used)

The type of the NAN Service Discovery frame the Publish function uses depends on the configuration given in the Publish command.

If the Publish instance has been created to generate unsolicited transmissions only, it requests the NAN Engine to transmit of Publish messages that are broadcasted. Each instance of the Publish function should generate those transmission requests based on the announcement period indicated in the Publish command. Figure 15 illustrates the data flow for the unsolicited Publish command.

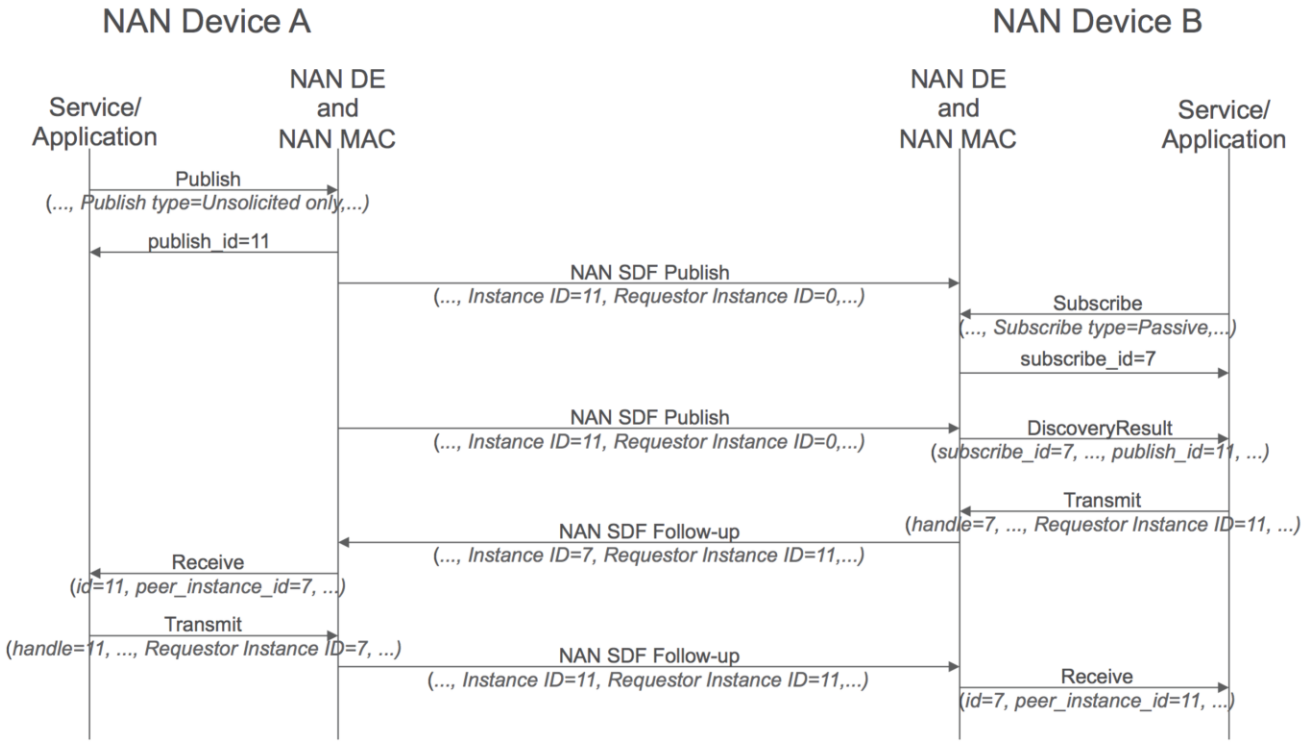


Figure 15. Unsolicited Publish command data flow

If the Publish instance has been created to generate only solicited transmissions, it shall request the NAN Engine to transmit Publish messages only when a Subscribe message that meets the trigger condition has been received (refer to section 4.1.3.1). Figure 16 illustrates the data flow for solicited Publish command.

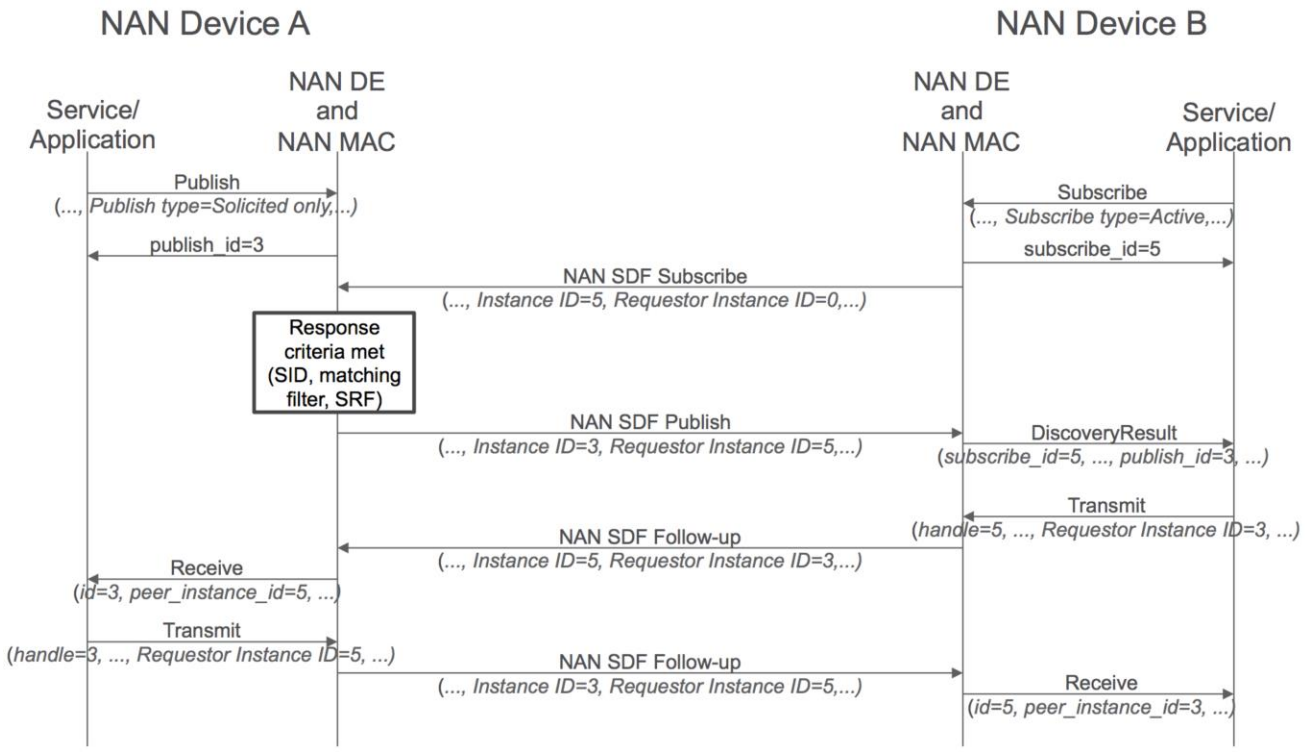


Figure 16. Solicited Publish command data flow

If the Publish instance has been created to generate both unsolicited and solicited transmissions, it shall request the NAN Engine to transmit both unsolicited and solicited Publish messages as described above.

Each instance of the Publish function may be configured to operate either with discoverability limited to close proximity or without any range limitation.

If the Publish instance has been created with discoverability limited to close proximity, it requests transmission of Publish messages with the Discovery Range Limited bit set to one (refer to section 9.5.4).

If the Publish instance has been created without any range limitation, it requests transmission of Publish messages with the Discovery Range Limited bit set to zero (refer to section 9.5.4).

4.1.3.1 Publish trigger condition

When an instance of the Publish function receives a Subscribe message from the Receive Control function, the Publish function instance checks whether the Subscribe message meets the trigger conditions. The Receive Control function (section 4.1.6) has already checked that the request packet contains a Hash Value for which the instance of the Publish function SID is configured.

If the Subscribe message contains a non-zero length Matching Filter, the instance of the Publish function checks whether the Matching Filter in the Subscribe message matches the values given for the instance of the Publish function. If there is a match between each element value in the Subscribe message and a value given for the instance of the Publish function, a trigger condition is met.

Each <length, value> pair in kth (k = 1 to number of <length, value> pairs in the matching filter field of the Service Descriptor Attribute) position in the Matching Filter field of the Service Descriptor Attribute in the Subscribe message is compared against the kth <length, value> pair in the matching_filter_rx.

- For a kth position <length, value> pair in the Matching Filter field of the Service Descriptor attribute with length = 0, a match is declared irrespective of the exact values of the kth <length, value> pair in the matching_filter_rx
- For a kth position <length, value> pair in the Matching Filter field of the Service Descriptor attribute with length > 0, a match is declared when the kth <length, value> pair in the matching_filter_rx is exactly equal to the kth position <length, value> pair in the Matching Filter field of the Service Descriptor attribute, or the kth <length, value> pair in the matching_filter_rx has length = 0

If the number of <length, value> pairs in the Matching Filter field of the Service Descriptor attribute is less than or equal to the number of <length, value> pairs in the matching_filter_rx, and there is a match declared for each <length, value> pair in the Matching Filter field of the Service Descriptor attribute, a trigger condition is met; otherwise, a trigger condition is not met.

If the Subscribe message contains a non-zero length Matching Filter that contains at least one <length, value> pair with length larger than zero, but the instance of the Publish function does not provide a matching_filter_rx value, a trigger condition is not met.

If the Subscribe message does not contain any non-zero length Matching Filter or the Subscribe message contains a non-zero length Matching Filter that does not include any <length, value> pair with length larger than zero, a trigger condition is met irrespective of the matching_filter_rx value given for the instance of the Publish function.

Some trigger condition examples are provided in Appendix H.

When a trigger condition is met, the instance ID obtained from the message is recorded and should be included in the Requestor Instance ID field of the Publish message when the NAN SDF Publish frame is transmitted as shown in Figure 16. Note that the Requestor Instance ID is set to 0x00 for unsolicited Publish messages.

If the Publish instance has been created with discovery limited to close proximity, it checks whether the Subscribe message was received with signal level that is higher than implementation specific threshold level RSSI_close_proximity. If the signal level of the received Subscribe message exceeds the threshold level, the discovery range trigger condition is met.

If the Publish instance has been created without discovery range limitation and the received Subscribe message has the Discovery Range Limited bit set to one, the Publish instance checks whether the Subscribe message was received with signal level that is higher than implementation specific threshold level RSSI_close_proximity. If the signal level of the received Subscribe message exceeds the threshold level, the discovery range trigger condition is met.

If the Publish instance has been created without discovery range limitation and the received Subscribe message has the Discovery Range Limited bit set to zero, all received Subscribe messages meet the discovery range trigger condition regardless of the reception signal level.

4.1.3.2 Publish updates

The Publish function may use the Service Update Indicator field in the SDEA to indicate the version of the service specific information corresponding to the publish instance, which may be conveyed by publish messages and/or FSD messages. If an instance of the Publish function is using the Service Update Indicator field in the SDEA, then the Publish function shall increment the Service Update Indicator, and update the SDEA, for every call to the UpdatePublish method.

4.1.4 Subscribe function

The Subscribe function operates as per Subscribe commands from services/applications through the Service Interface. When the Subscribe command is executed, it generates an instance of the Subscribe function which may run for a given time interval or until the first DiscoveryResult event, whichever occurs first. Each instance of the Subscribe function has a subscribe_id that uniquely identifies the instance locally. The subscribe_id is also used across devices in NAN discovery to uniquely identify an instance of a service on a specific device. Each instance of the Subscribe function runs independently and the number of concurrently supported instances of the Subscribe function is implementation dependent. The following description applies to each instance of the Subscribe function separately.

Each instance of the Subscribe function may be configured to operate either in passive or in active mode.

In the passive mode, the Subscribe function does not request transmission of any Subscribe messages, but checks for matches in received Publish messages.

In the active mode, the Subscribe function additionally requests transmission of Subscribe messages and processes Publish messages.

When a Publish message discovery frame containing the Service ID given by the Subscribe function is received, the Matching Filter field of the Service Descriptor attribute in the Publish message is matched against the matching_filter_rx parameter of the corresponding Subscribe function as follows.

Each <length, value> pair in kth position in the matching_filter_rx (k = 1 to number of <length, value> pairs in the matching_filter_rx) is compared against the kth <length, value> pair in the Matching Filter field of the Service Descriptor attribute in the Publish message.

- For a k^{th} position <length, value> pair in the matching_filter_rx with length = 0, a match is declared irrespective of the exact values of the k^{th} <length, value> pair in the Matching Filter field of the Service Descriptor attribute
- For a k^{th} position <length, value> pair in the matching_filter_rx with length > 0, a match is declared when the kth <length, value> pair in the Matching Filter field of the Service Descriptor attribute is exactly equal to the k^{th} position <length, value> pair in the matching_filter_rx, or the k^{th} <length, value> pair in the Matching Filter field of the Service Descriptor attribute has length =0

A DiscoveryResult event is declared if the number of <length, value> pairs in the matching_filter_rx is less than or equal to the number of <length, value> pairs in the Matching Filter field of the Service Descriptor attribute in the Publish message; and a match is declared on each <length, value> pair in the matching_filter_rx; otherwise, a DiscoveryResult event is not declared.

If the Publish message contains a non-zero length Matching Filter, but the instance of the Subscribe function does not provide a matching_filter_rx value, a DiscoveryResult event is declared.

If the Publish message does not contain any non-zero length Matching Filter, a DiscoveryResult event is only declared if the Subscribe function does not provide a matching_filter_rx value or the Subscribe function provides a matching_filter_rx that does not include any <length, value> pair with length larger than zero; otherwise, a DiscoveryResult event is not declared.

Some examples on DiscoveryResult event declaration are provided in Appendix H.

Each instance of the Subscribe function may be configured to operate either with discovery limited to close proximity or without a discovery range limitation.

If the active mode Subscribe instance has been created with discovery limited to close proximity, it requests transmission of Subscribe messages with the Discovery Range Limited bit set to one (refer to section 9.5.4).

If the active mode Subscribe instance has been created without discovery range limitation, it requests transmission of Subscribe messages with the Discovery Range Limited bit set to zero (refer to section 9.5.4).

If the Subscribe instance has been created with discovery limited to close proximity, it checks whether a Publish message was received with signal level that is higher than the implementation specific threshold level RSSI_close_proximity. If the signal level of the received Publish message exceeds the threshold level, the discovery range limitation trigger condition is met.

If the Subscribe instance has been created without discovery range limitation and the received Publish message has the Discovery Range Limited bit set to one, the Subscribe instance checks whether the Publish message was received with a signal level that is greater than implementation specific threshold level RSSI_close_proximity. If the signal level of the received Publish message exceeds the threshold level, the discovery range limitation trigger condition is met.

If the Subscribe instance has been created without discovery range limitation and the received Publish message has the Discovery Range Limited bit set to zero, all received Publish messages regardless of the reception signal level meet the discovery range limitation trigger condition.

When the discovery range limitation trigger condition is met, a DiscoveryResult event shall be sent (refer to section 4.1.1.2) if other conditions for the event transmission are met.

4.1.5 Transmit Control function

The Transmit Control function is responsible for forming a NAN Service Discovery frame from one or more Service Descriptors from instances of the Publish function and from instances of the Subscribe function.

Additionally, the Transmit Control function generates a NAN Service Discovery frame from one or more Follow-up messages from the Follow-up function.

Once the Transmit Control function has a NAN Service Discovery frame ready for transmission, it requests the NAN MAC to transmit the frame.

4.1.6 Receive Control function

The Receive Control function is responsible for decoding NAN Service Discovery frames, decoding individual Service Descriptor attributes and related NAN Service Discovery protocol messages from received NAN Service Discovery frames, filtering individual Service Descriptor attributes, and after filtering providing individual Service Descriptor attributes either to an instance of the Publish function, to an instance of the Subscribe function or to the Follow-up function.

The Receive Control function filters those Service Descriptor attributes and related NAN Service Discovery protocol messages that contain a Hash Value that does not match with any of the Hash Values of published or subscribed service name. Those Subscribe messages that contain a Hash Value that matches with a Hash Value of a published service name are provided to the corresponding instance of the Publish function for further processing. Those Publish messages that contain a Hash Value that matches with a Hash Value of a subscribed service name are provided to the corresponding instance of the Subscribe function for further processing. Those Follow-up messages that contain a Hash Value that matches with a Hash Value of a published or a subscribed service name are provided to the Follow-up function for further processing.

4.1.7 Follow-up function

The Follow-up function provides means for services/applications to transmit and receive service specific information to and from a NAN Device. Service Hash based filtering is used upon reception and the use of filtering requires an instance of the Publish function or an instance of the Subscribe function to be active; therefore, a Follow-up shall be requested with a valid publish_id or a subscribe_id.

Upon transmission, the Follow-up function generates a Follow-up message from the elements received from the service/application in the Transmit Method and requests transmission of the message from the Transmit Control function. There are no specific rules to be applied to transmission requests.

The service_specific_info from the Follow-up Transmit command are put into either the Service Info field of the SDA or the Service Info field of the SDEA.

NOTE: Due to the size limit of the Service Info field of the SDA, if the service_specific_info is longer than 255 bytes, the Service Info field of the SDEA should be used).

Upon reception, the Follow-up function just passes the information from the Service Info field in either the SDA or SDEA of the received Follow-up message to the service/application.

In the follow-up message generated for transmission by the Follow-up function, the Requestor Instance ID shall be set to the instance id received in the Publish or Subscribe message that triggered the follow up function.

With secure NAN pairing and verification, the Follow-up function may be used to provision an IGTK, and a BIGTK to utilize multicast management frame protection, Beacon integrity protection. Such protection does not require a NAN Data Path setup.

4.1.8 NAN Control function

The NAN Control function is responsible for configuring four functions of the NAN Discovery Engine and the NAN MAC, namely Publish, Subscribe, Follow-up request(s), and Filtering.

4.1.9 NAN Filtering function

There are two parts to NAN Filtering Function:

1. Matching Filter (MF)
2. Service Response Filter (SRF)

4.1.9.1 Matching Filter

The Matching Filter may be used by a sender of a NAN Service Discovery frame to provide additional parameters for the Service ID in the Service Descriptor attribute. The Matching Filter enables the receiver of a NAN Service Discovery protocol message to accept or reject NAN Service Discovery frames that correspond to a Service Descriptor. The format of the Matching Filter is a flexible sequence of length value fields as indicated in section 9.5.4. The fields of the Matching Filter are populated through the matching_filter_tx variable of the corresponding Publish (section 4.1.1.1) and Subscribe (section 4.1.1.1) functions.

4.1.9.2 Service Response Filter

The Service Response Filter field in the Service Descriptor attribute (section 9.5.4) allows the sender of a NAN Service Discovery frame to indicate which NAN Devices should or shall not respond to the NAN Service Discovery protocol message. A Service Response Filter is created on a per service basis. A potential respondent determines if it is indicated in the Address Set field as follows:

- If the SRF Type field is set to zero, the potential respondent determines if its 6 octet MAC address is equal to any one of the addresses in the list of NAN Interface Addresses of the SRF attribute Address Set field
- If the SRF Type field is set to one, the potential respondent uses the procedure in section 10.3 to determine if it is listed in the Address Set field

If the Include bit in the SRF Control field is one, a potential respondent that is indicated in the Address Set field transmits a response to the received NAN Service Discovery protocol message.

If the Include bit in the SRF Control field is zero, a potential respondent that is indicated in the Address Set field shall not transmit a response to the received NAN Service Discovery protocol message.

4.2 Power Efficient Service Discovery

If a value for Awake DW Interval (p) in configuration_parameters is specified for a service, the NAN Device shall wake up at least at the Discovery Windows in which TSF[22:19] mod p is set to zero to publish or subscribe the service. Note that TSF[22:19] represents the Bit 19 to Bit 22 of the TSF.

For example, if the Awake DW Interval is set to one, the NAN Device publishing/subscribing the service shall wake up at every Discovery Window; if the Awake DW Interval is set to 8, the NAN Device publishing/subscribing the service shall wake up at least at Discovery Windows in which the values “TSF[22:19] mod 8” are set to zero.

If multiple awake DW intervals are specified for different services that need to be subscribed or published, the NAN Device shall use the smallest Awake DW Interval to calculate the awake DWs.

NOTE: A NAN Device in a Master role or in a Non-Master role and Sync state needs to be awake in all DWs to transmit NAN Synchronization Beacons.

4.3 Further Service Discovery

A publisher may select to use either the Follow-up function (as specified in section 4.1.7) or the GAS based NAN Further Service Discovery function (as specified in Appendix I) to provide further service discovery support.

The publisher uses the Further Service Discovery flag and the Further Service Discovery function parameter in the publish method to indicate its further service discovery function for a supported service.

If the publisher selects to use the Follow-up function to provide further service discovery support, it shall set the FSD Required flag to one and the FSD with GAS field to zero in the corresponding SDEA included in its publish messages.

When a subscriber receives the publish messages, it shall report the publisher's FSD support and function for the corresponding service in the DiscoveryResult event.

If a publisher indicates FSD support using GAS for a service, a subscriber calls the GASScheduleRequest method to request the NAN Scheduler to secure sufficient NDL CRBs for subsequent GAS message exchanges.

If there are not sufficient NDL CRBs between the subscriber and the publisher, the subscriber may initiate the NDL Schedule setup or update with the publisher, as specified in section 6.2.3.4.

In response to a received GASScheduleRequest call, the GASScheduleConfirm event will be issued to report the result of the GAS scheduling.

If the GASScheduleConfirm event reports the status as "Accepted", the subscriber may start exchanging GAS message with the publisher.

Figure 17 shows the procedure for GAS based NAN Further Service Discovery.

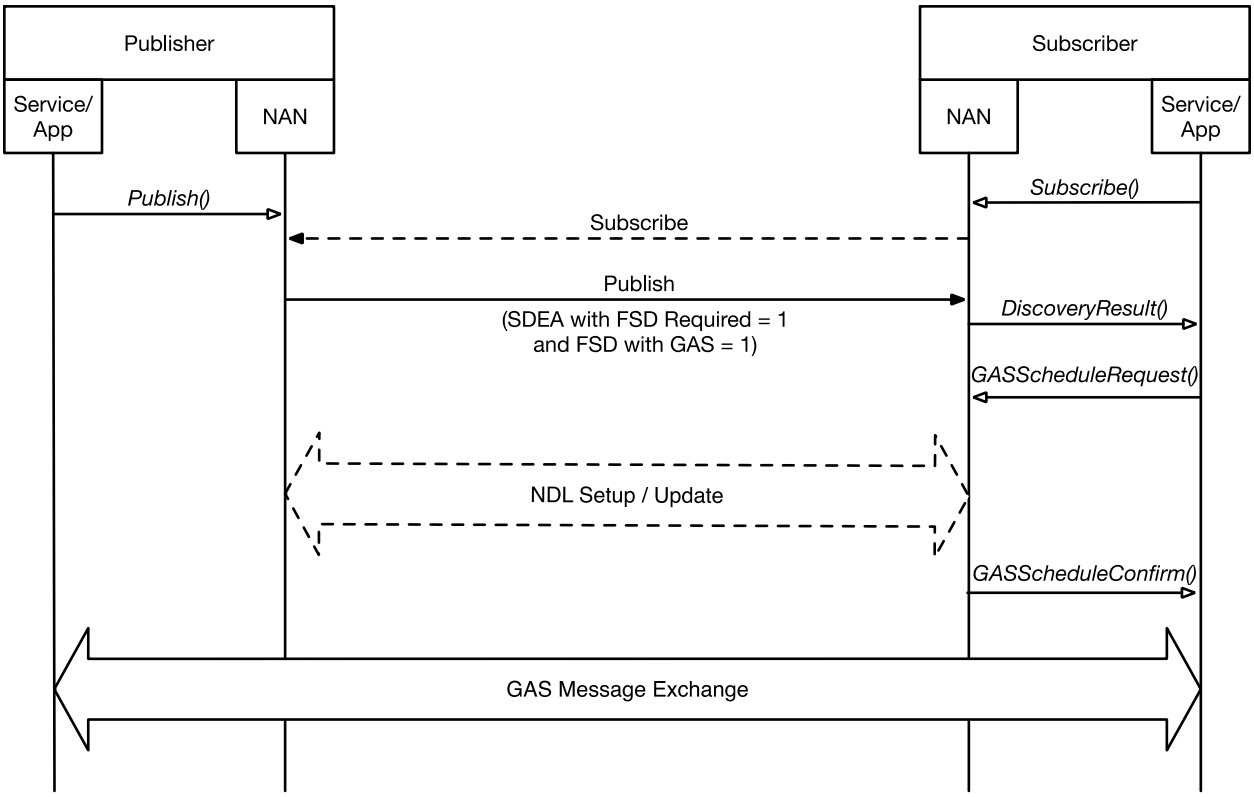


Figure 17. NAN Further Service Discovery using GAS

4.4 Conveying detailed service information using the Generic Service Protocol

A service publisher may use the Generic Service Protocol to convey detailed service information to a subscriber, by

- Including a Service Info field in the SDEA of a publish or follow-up message, and
  Ssetting the OUI subfield of the Service Info field to 0x50-6F-9A (Wi-Fi Alliance specific OUI), and
- Setting the Service Protocol Type subfield of the Service Info field to 2 (Generic), and
- Including one or more of the sub-attributes below in the Service Specific Info subfield of the Service Info field:
  - Service Name sub-attribute
  - Name of Service Instance sub-attribute
  - TextInfo sub-attribute

- UUID sub-attribute
- BLOB sub-attribute
- Vendor Specific Info sub-attribute

As an example, a service publisher may convey detailed service information by using the following sub-attribute combination:

- Service Name sub-attribute
- Name of Service Instance sub-attribute
- TextInfo sub-attribute

The service publisher may include all the sub-attributes in a single Publish message to facilitate fast and efficient NAN Service Discovery when permitted by the channel access rules in section 3.5.

4.5 Unsynchronized Service Discovery

Unsynchronized Service Discovery (USD) is a mechanism for devices to discover the services that have been made discoverable on new devices that enter the RF environment, without requiring synchronization between the devices described in section 3.

The publisher in USD is discoverable by the subscriber in USD.

The publisher in USD is discoverable by the active mode subscriber in NAN Discovery with NAN Synchronization (see section 3).

When USD is used only for NAN Service Discovery, the NAN peer communication ends at the end of the Unsynchronized Discovery. When a service requires more than NAN Service Discovery (e.g., NAN ranging or NAN Data Path), the NAN Synchronization is conducted.

USD shall use Service Info field in the SDEA of a Publish and Follow-up message to convey the service specific information because it supports larger size of service information.

4.5.1 Publisher behavior in USD

The publisher shall create a Publish instance for both solicited and unsolicited transmissions of the Publish messages. The publisher should populate fields of the Matching Filter (see section 4.1.9) in the Publish message through matching_filter_tx variable of the corresponding Publish (see section 4.1.1.1). The publisher shall begin operation in the Single channel Publish state. The publisher shall iterate between the Single channel Publish state and the Multiple channels Publish state until the USD is terminated.

The publisher in each Single channel Publish state shall operate only in the defaultPublishChannel. The dwell period in each Single channel Publish state is $N * 100$ TU (Transmission Unit). N is an integer within range [Nmin, Nmax]. The publisher randomly selects N for each Single channel Publish state.

The publisher in each Multiple channels Publish state shall operate in one or more channels in the publishChannelList. The dwell period in each Multiple channels Publish state is $M * 100$ TU. M is an integer within range [Nmin, Nmax]. The publisher randomly selects M for each Multiple channels Publish state. It is up to implementation to divide the dwell period in each Multiple channels Publish state between the channels in the publishChannelList. The publisher may publish on a subset of channels in the publishChannelList in each Multiple channels Publish state. The minimum amount of time spent on a channel in each Multiple channels Publish state is 100 ms.

The default values of Nmin, Nmax, Mmin, and Nmax are 5, 10, 5 and 10, respectively or be based on the USD configuration (see section 4.1.1.1) if provided by the Service layer. It is recommended that $Nmin >= 5$ and $Mmin >= 5$ to facilitate discoverability of the publisher in USD by the active mode subscriber in NAN Discovery with NAN Synchronization.

The randomness in the dwell period in each Single channel Publish state and Multiple channels Publish state is to avoid a situation where the publisher and the subscriber are in lockstep and thus will never discover each other. The publisher shall iterate between the Single channel Publish state and Multiple channels Publish state on expiry of their respective dwell periods.

The publisher in USD shall not send NAN Discovery Beacon and NAN Synchronization Beacon frames. The publisher shall always stay awake in the USD.

The publisher uses the Further Service Discovery flag and Further Service Discovery function parameter in the publish method to indicate its further service discovery function for supported service. The publisher shall set the FSD Required flag to one and the FSD with GAS field to zero in the corresponding SDEA included in its publish messages.

When the publisher receives a Follow-up message without Service Specific Info field in SDEA from the subscriber, if a Receive event is declared, the publisher shall set the pauseStateTimeout to 60 seconds, after receiving the Follow-up message without Service Specific Info field in SDEA that caused the Receive event declaration.

When the publisher receives a Subscribe message, if a Replied event is declared, the publisher shall set the pauseStateTimeout to 60 seconds, after receiving the Subscribe message that caused the Replied event declaration.

While the pauseStateTimeout is counting down towards its expiry:

- The publisher shall stay on the current channel in the current state
- The publisher shall ignore the dwell period on the current channel in the current state
- The publisher shall ignore any Follow-up message sent by another subscriber that is different from the subscriber that triggered the pauseStateTimeout count down
- The publisher shall ignore any Follow-up message without Service Specific Info field in SDEA that is sent by the subscriber that triggered the pauseStateTimeout count down. The publisher shall not reset the pauseStateTimeout
- The publisher shall ignore any Subscribe message sent by another subscriber that is different from the subscriber that triggered the pauseStateTimeout count down
- The publisher receives a Subscribe message that is sent by the subscriber that triggered the pauseStateTimeout count down, if a Replied event is declared, the publisher shall not reset the pauseStateTimeout
- The publisher whose pauseStateTimeout is set because of reception of Subscribe message that caused a Replied event declaration, shall send solicited Publish messages periodically to the subscriber that triggered the pauseStateTimeout count down until the publisher receives at least one Follow-up message with Service Specific Info field in SDEA from the subscriber that triggered the pauseStateTimeout count down. How often the solicited Publish message is sent in this case is implementation dependent although the recommendation is every 100 TUs. The publisher shall not reset the pauseStateTimeout with each Replied event. This behavior facilitates publisher in USD to be discovered by the active subscriber in NAN Discovery with NAN Synchronization
- The publisher shall not send unsolicited Publish messages
- The publisher receives at least one Follow-up message with Service Specific Info field in SDEA from the subscriber that triggered the pauseStateTimeout count down, if a Receive event is declared, the publisher shall reset the pauseStateTimeout such that it expires when the USD is terminated

If the publisher does not receive a Follow-up message with Service Specific Info field in SDEA from the subscriber that triggered the pauseStateTimeout count down and the pauseStateTimeout expires, then the publisher shall return to the Single channel Publish state and continue iterating between the Single channel Publish state and Multiple channels Publish state as described above.

4.5.2 Subscriber behavior in USD

The subscriber shall create a Subscribe instance that is configured to operate either in passive or active mode. The subscriber shall choose a channel using implementation specific methods at the beginning of USD and this channel shall remain the same until the USD is terminated. This channel shall be in the 2.4 GHz frequency band or the 5 GHz frequency band, per regulation in the geographical location or this channel be selected from the USD configuration (see section 4.1.1.1) if provided by the Service layer, per regulation in the geographical location.

How often the subscriber is present on this channel and each dwell time on this channel is implementation dependent. It is recommended that subscriber use defaultPublishChannel for USD.

When the passive subscriber receives the unsolicited Publish message, if a DiscoveryResult event is declared, the subscriber shall send at least one Follow-up message without Service Specific Info field in SDEA to the publisher. It is recommended that the subscriber send the Follow-up message without Service Specific Info field in SDEA to the publisher no later than 80 ms after receiving the Publish message that caused DiscoveryResult event declaration. The purpose of the Follow-up message without Service Specific Info field in SDEA is to temporarily pause the publisher on its

current channel and its current state for pauseStateTimeout. The subscriber may send more Follow-up messages with Service Specific Info field in SDEA to continue USD with the publisher to which it sent the Follow-up message without Service Specific Info field in SDEA.

When the active subscriber receives the solicited Publish message, if a DiscoveryResult event is declared, then the subscriber may send one or more Follow-up messages with Service Specific Info field in SDEA to the publisher to continue USD with the publisher. The Subscribe message temporarily pauses the publisher on its current channel and its current state for pauseStateTimeout.

When the active subscriber receives the unsolicited Publish message, if a DiscoveryResult event is declared, then the subscriber shall send a Subscribe message. It is recommended that the subscriber send the Subscribe message no later than 80 ms after receiving the unsolicited Publish message that caused DiscoveryResult event declaration.

4.5.3 Operating channels in USD

The defaultPublishChannel is the channel 6 (2.437 GHz) in the 2.4 GHz frequency band or be based on the USD configuration (see section 4.1.1.1) if provided by the Service layer, per regulation in the geographical location.

The publishChannelList shall contain all the 20 MHz channels in the 2.4 GHz frequency band, per regulation in the geographical location and if the publisher supports USD in the 5 GHz frequency band, then the publishChannelList also contains all the 20 MHz channels in the 5 GHz frequency band, per regulation in the geographical location or be based on the USD configuration (see section 4.1.1.1) if provided by the Service layer, per regulation in the geographical location. How a publisher determines its geographical location is out of scope of this specification.

4.5.4 Termination of USD

CancelPublish and CancelSubscribe methods are used to terminate USD at the publisher and the subscriber, respectively.

4.5.5 USD Diagram

This section has sequence diagrams for illustration of USD. These are provided as examples and do not cover all possible situations.

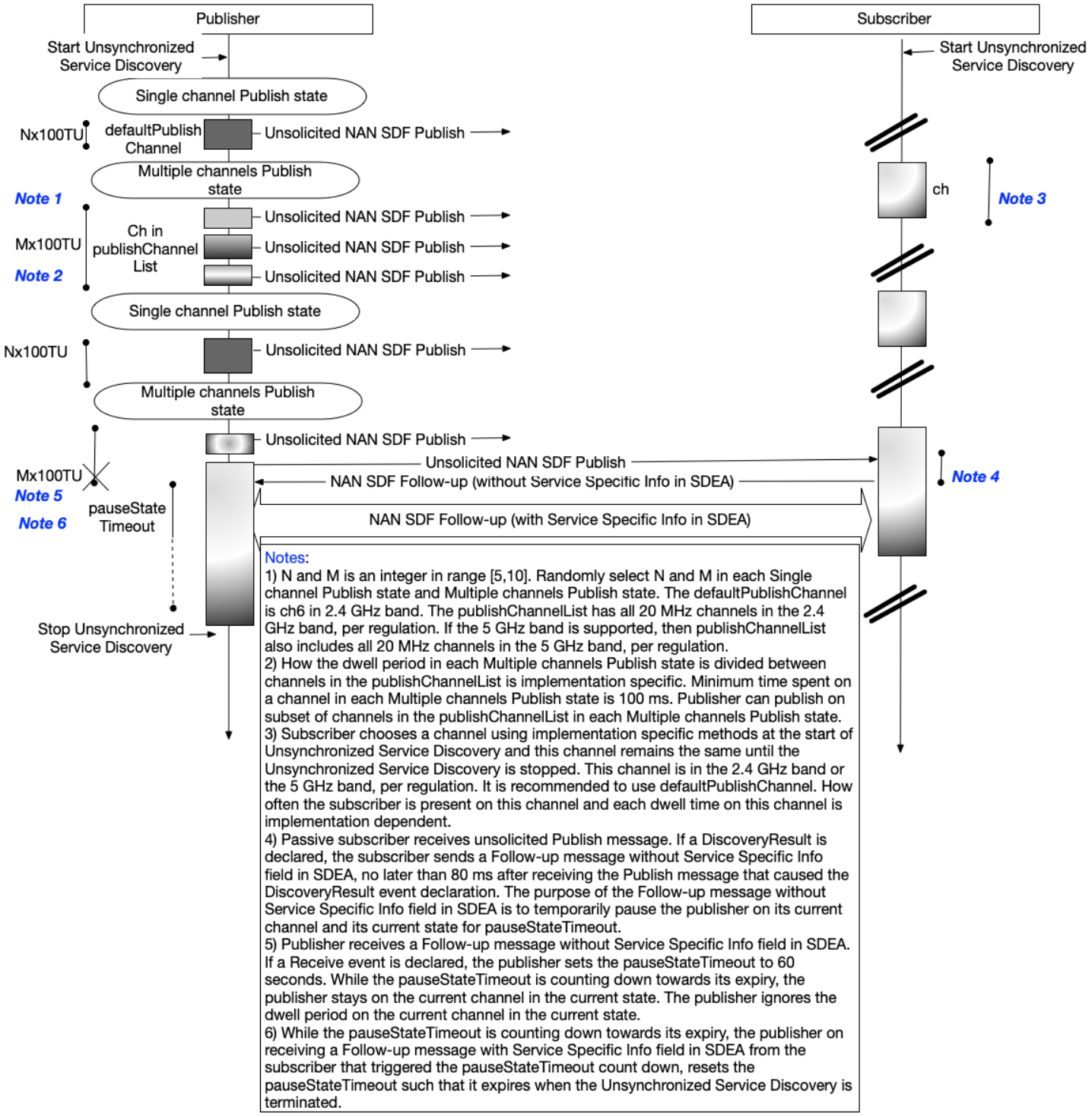


Figure 18. Example of passive subscriber in USD hearing an unsolicited Publish message from a publisher in USD

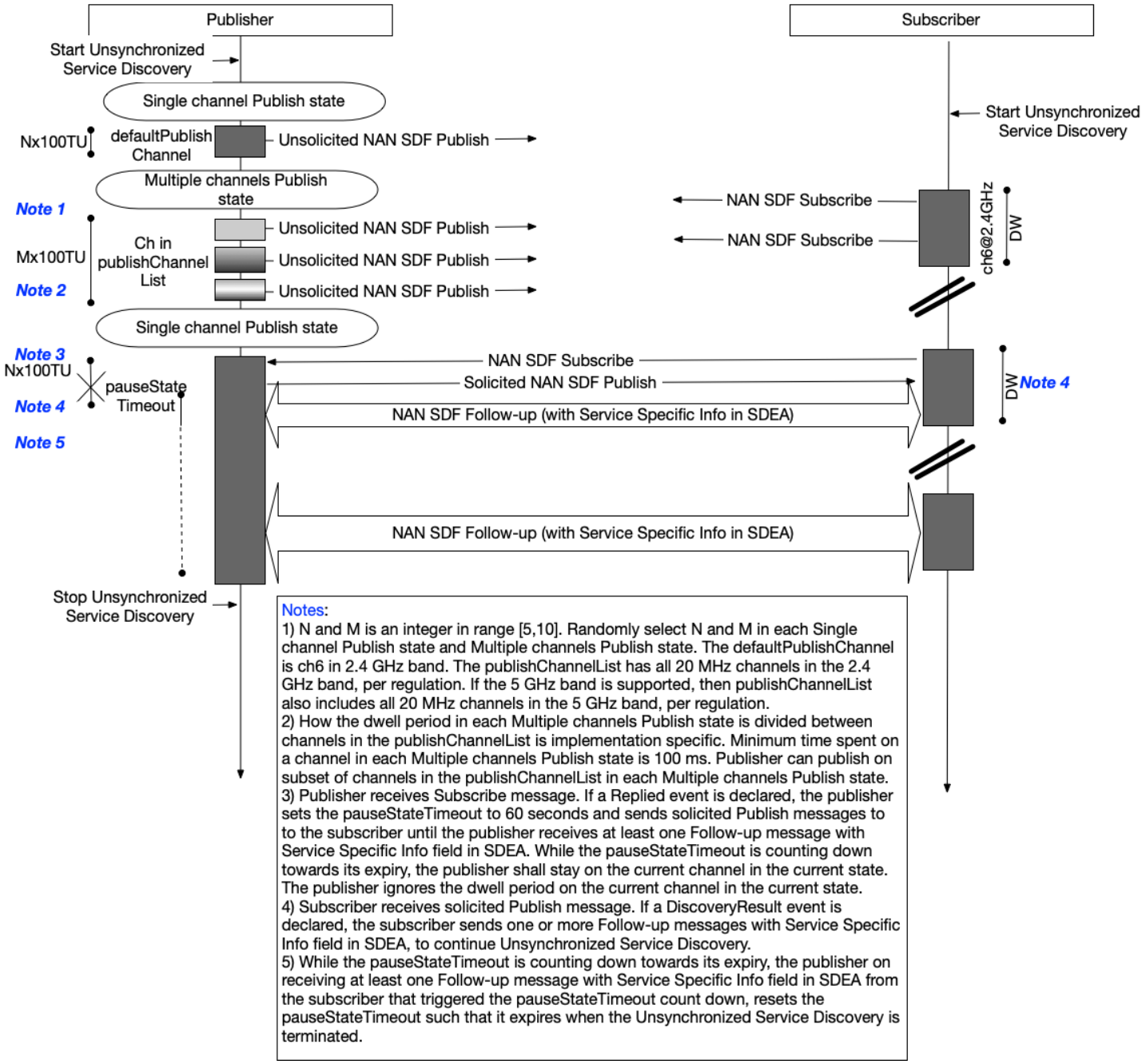


Figure 19. Example of active subscriber in NAN Discovery with NAN Synchronization hearing a solicited Publish message from a publisher in USD

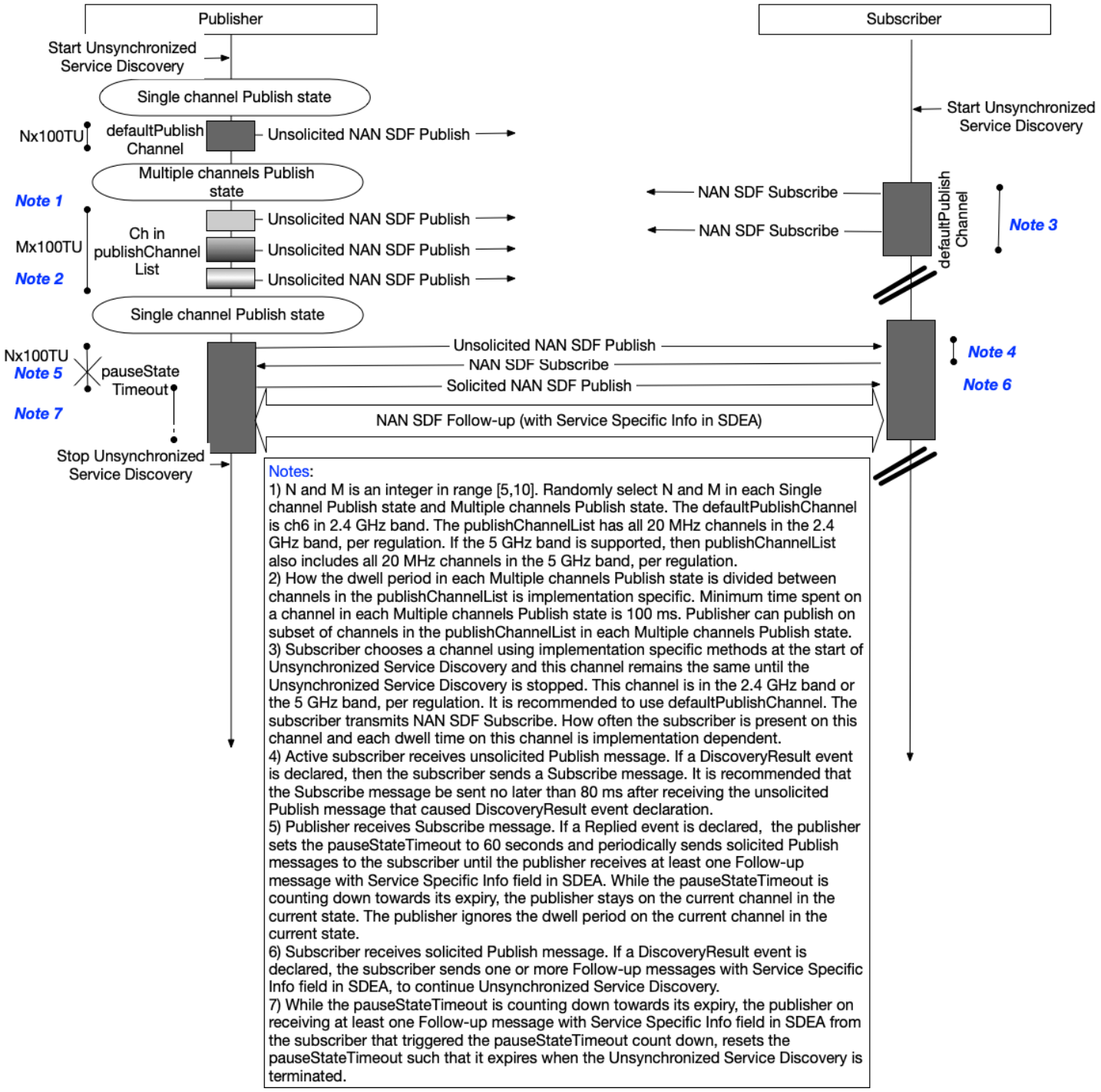


Figure 20. Example of active subscriber in USD hearing an unsolicited Publish message from a publisher in USD.

5 NAN Scheduler

The NAN Scheduler is responsible for establishing, maintaining, and terminating Wi-Fi radio resource schedules for NAN operations. It is also responsible for coordinating concurrent NAN and Non-NAN operations.

The NAN Scheduler in each NAN Device publishes its potential and committed availability schedules to interested peers in a same NAN Cluster, and collects the peers' potential and committed availability schedules.

A NAN Device's availability schedules include DWs, Further Availability Windows (FAWs), and Unaligned Windows (ULWs). Committed FAWs may be further refined by the device's S3 for a given NDP operation.

A NAN Device may transmit NAN frames to a peer NAN Device in a same NAN Cluster during the peer device's committed DW or committed FAW, except for those (or partial of those) exempted by its ULWs or canceled for power saving. The transmission shall be permitted by the medium access rules in these windows.

A NAN Device may also transmit NAN frames to a peer NAN Device in a same NAN Cluster during the peer device's available ULWs (refer to section 5.1.3).

If a NAN Device is available in more than one channel simultaneously in one committed FAW or ULW, and it sets Bit 2 (Simultaneous NDP data reception) to value of zero in the Capabilities field of the Device Capability attribute, a peer NAN Device shall transmit NAN data frames, which belong to the same NDI pair between the two NAN Devices, in the same channel within the FAW or ULW.

A NAN Device shall be available at the start of its each committed FAW and committed DW. Note: A NAN Device can switch channel if required before the start of committed FAW or committed DW.

The S3 mechanism is not applicable to any committed DW and NDC Schedule.

A NAN Device should include its Max Channel Switch Time in the Device Capability attribute to indicate the duration of channel switching where it is not available to transmit and receive.

A NAN Device providing Max Channel Switch Time shall incur this channel switch outage time immediately before the next channel switch. Note: If a device needs to be in a new channel starting at reference point A, then the NAN Device incur this channel switch outage time immediately before the point A.

A NAN Device should make use of the peer's Max Channel Switch Time to stop transmitting when the peer is not available during channel switch time.

5.1 NAN Availability Schedule Indications

5.1.1 Committed DW Indication

A NAN Device indicates the Committed DWs by:

- Including the Device Capability attribute in a NAN management frame; and
- Setting the Committed DW Info field of the Device Capability attribute according to its DW wakeup schedule

A NAN Device shall be present during its Committed DWs, except for those (or partial of those) exempted by its ULWs.

5.1.2 FAW Indication

A NAN Device indicates the FAWs it will be present for NAN or Non-NAN operations by including the following attributes in a NAN management frame:

- One or more Further Availability Map attributes
- One or more NAN Availability attributes
- NAN ASI attributes associated with NAN Operations
- NAN ASI attributes associated with Non-NAN Operations

The Further Availability Map attribute and the NAN Availability attribute serve similar purpose. The NAN Availability attribute is designed to replace the Further Availability Map attribute. Therefore, the use of the Further Availability Map attribute is obsolete.

5.1.2.1 NAN Availability attribute

The NAN Availability attribute is used by a NAN Device to indicate Committed FAWs that the NAN Device will be present, as well as not-yet committed, but preferred, FAWs for upcoming NAN operations.

A NAN Device operating simultaneously on multiple bands or channels shall include more than one NAN Availability attribute in a NAN management frame, in which case, the NAN Availability attribute shall indicate conditional or committed availability on two or more different primary channels during at least one common NAN Slot.

A NAN Device shall include at most one NAN Availability attribute in a NAN management frame, unless:

- It uses simultaneous operations on multiple bands or channels; or
- It needs to indicate different sets of capabilities for different radios, bands, or channels

A NAN Device should use the least possible number of NAN Availability attributes in a NAN management frame to describe its availability.

When a NAN management frame includes multiple NAN Availability attributes,

- Each NAN Availability attribute shall be identified by a different Map ID; and
- All NAN Availability attributes shall share the same Sequence ID and the same schedule change flag values in the Attribute Control fields

The schedule change flags in the Attribute Control field shall be set when corresponding schedules or schedule attributes are changed, compared with those in the last schedule advertisement. The Sequence ID value shall be incremented by one if any schedule change flag in the Attribute Control field is set to one.

Each NAN Availability attribute shall include at least one Availability Entry, and may include more than one Availability Entry.

Each Availability Entry specifies one or a sequence of FAWs, which are confined by following parameters:

- Time windows, specified by the Time Bitmap Control field, the Time Bitmap Length field, the Time Bitmap field
- A band/channel or a band/channel list, specified by the Band/Channel Entry List field
- Number of spatial streams, specified by the Rx Nss subfield in the Entry Control field

An Availability Entry shall specify FAWs within a time period starting from the beginning of the previous DW0, and lasting any length from 1 to 512 NAN Slots. The FAWs specified in that time period may be repeated.

The channel or channel list and the number of spatial streams specified by an Availability Entry shall be applied to all FAWs indicated by the same Availability Entry.

the Time Bitmap Control field, the Time Bitmap Length field, and Time Bitmap field may be omitted according to Table 97.

An Availability Entry shall be set as one or two of following availability types:

- Committed type: The NAN Device shall be present at associated FAWs, except for those (or partial of those) exempted by ULWs (refer to section 5.1.3) or canceled for power savings
- Potential type: The NAN Device prefers to be present at associated FAWs, if needed
- Conditional type: The NAN Device proposes to be present at associated FAWs during schedule negotiation, and shall be present at the portions of the FAWs accepted by the peer NAN Device, except for those (or partial of those) exempted by ULWs (refer to section 5.1.3). This type shall not be present in NAN frames when there is no negotiation, such as in NAN SDF frames

Table 9 summarizes the allowed availability types for an Availability Entry, and their relationship with the Channel Entries List field in the same Availability Entry.

Table 9. Availability Entry types and Channel Entries

Allowed Availability types			Channel Entries list field	
Committed	**Potential**	**Conditional**	**Type**	**Band or Channel Entries**
Yes	No	No	Channel (1)	Only one channel entry, one channel and one primary channel
No	Yes	No	Band (0) or Channel (1)	One or more band or channel entries indicating one or more bands, or channels and primary channels
No	No	Yes	Channel (1)	Only one channel entry, one channel and one primary channel
Yes	Yes	No	Channel (1)	One or more channel entries: The first channel entry shall contain only one channel and one primary channel, and indicate the Committed FAW channel only. The remaining channel entries may contain one or more channels and primary channels, and indicate the potential FAW channels, which are not committed
No	Yes	Yes	Channel (1)	One or more entries: The first channel entry shall contain only one channel and one primary channel, and indicate the conditional FAW channel only. The remaining channel entries may contain one or more channels and primary channels, and indicate the potential FAW channels, which are not conditional.

The Conditional and Committed FAWs indicated by one NAN Availability attribute shall not conflict with each other. Two Committed or Conditional FAWs conflict with each other if, at the same point in time, these two FAWs associate with different primary channels.

The value of the Usage Preference subfield only applies to Potential FAWs.

A NAN Device is assumed to be potentially unavailable at a NAN Slot on a band/channel, unless:

- It explicitly indicates its committed or conditional availability at the NAN Slot on the channel, by including a corresponding Committed or Conditional Availability Entry; or
- It explicitly indicates its potential availability at the NAN Slot on the band/channel, by including a corresponding Potential Availability Entry with the Usage Preference subfield set to a Non-Zero value

A NAN Device may explicitly indicate its potential unavailability on certain channel(s) by including one or more Potential Availability Entries with the Usage Preference subfield set to zero, in which case, the Potential Availability Entries shall have the Time Bitmap Present subfield set to zero, and shall include the Channel Entries List field with at least one Channel Entry.

A Potential Availability Entry is considered to conflict with another Potential Availability Entry in a same NAN Availability attribute if both entries apply to a same NAN Slot on a same channel, but indicate different Usage Preference values:

- A Potential Availability Entry with the Channel Entries List may conflict with another Potential Availability Entry with the Band Entries List; in which case, the Usage Preference of the Potential Availability Entry with the Channel Entries List takes precedence
- A Potential Availability Entry with the Channel Entries List shall not conflict with another Potential Availability Entry also with the Channel Entries List

If a NAN Device uses a Potential Availability Entry to indicate its potential unavailability on a narrow bandwidth channel (e.g., a 20 MHz channel), it shall be considered to be potentially unavailable on all wider bandwidth channels (e.g., 40 MHz, 80 MHz, and 160 MHz channels) that include the narrow bandwidth channel.

Table 10 shows an example to use the Potential Availability Entries.

Table 10. Potential Availability example

Potential Availability Entries	Corresponding fields	Note
First Entry	Usage Preference = 1	

Potential Availability Entries	Corresponding fields	Note
	Time Bitmap Present = 0	Potential available on all channels on both 2.4 GHz and 5 GHz bands
	Band Entry List = 2.4 GHz and 5 GHz bands	
Second Entry	Usage Preference = 0	Potential unavailable on DFS channels, which takes precedence on the First Entry
	Time Bitmap Present = 0	
	Channel Entry List = all channels under Operating Class 118 and 121	
Third Entry	Usage Preference = 3	Potential available with strong preference in a FAW on Channel 36, which takes precedence on the First Entry
	Time Bitmap Present = 1 Bit Duration = 0 (16 TU) Offset = 24 (*16TU) Period = 3 (512 TU) Time Bitmap Length = 1 octet Time Bitmap = 0xFF	
	Channel Entry List = Channel 36	

Figure 21 shows an example of a NAN Device capable of simultaneous operation, and thus using two NAN Availability attributes to indicate its further availability schedules.

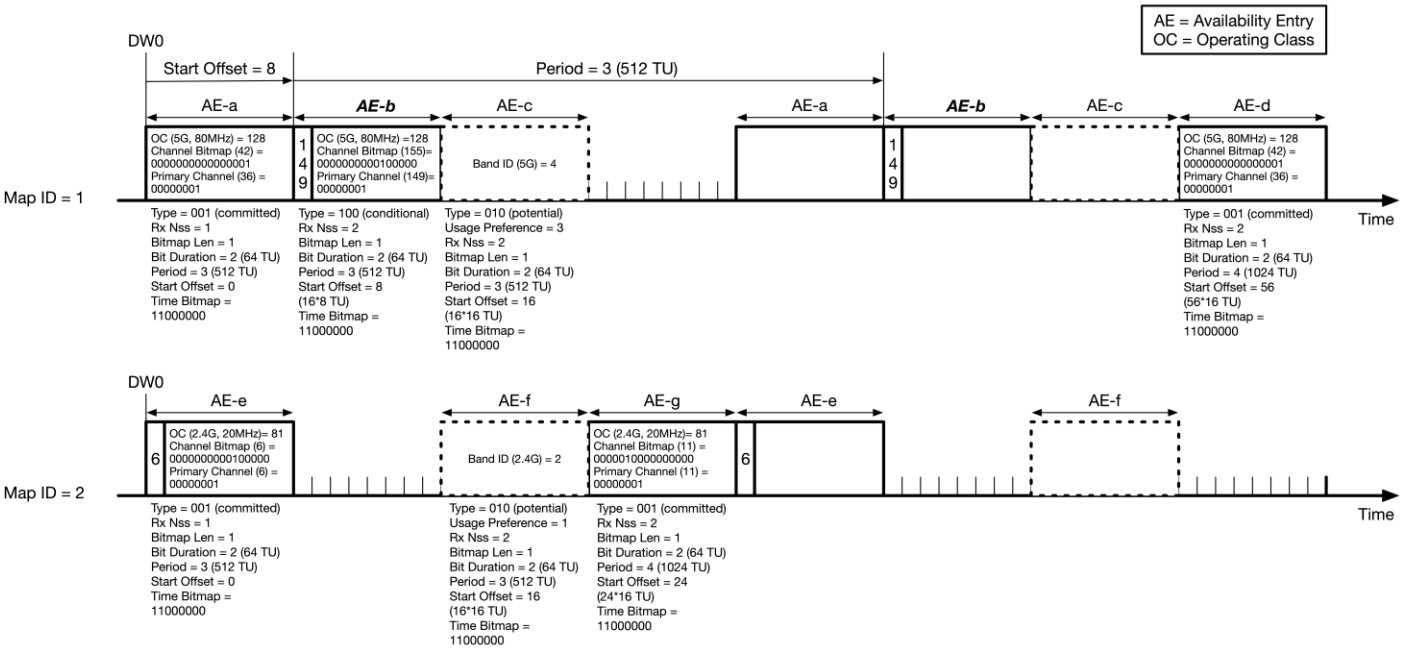


Figure 21. NAN Availability attribute example

5.1.2.2 NAN Aligned Schedule Indication attributes

NAN Aligned Schedule Indication (ASI) attributes refer to those attributes that contain the Aligned Schedule Indication (ASI). The ASI includes one or multiple schedule entries as specified in Table 104. In each schedule entry:

- The values of the Time Bitmap Control field, Time Bitmap Length field, and the Time Bitmap field indicate the time parameters of the FAWs associated with the NAN operation schedules.
- The value of the Map ID field indicates the NAN Availability attribute that provides other operation parameters of the FAWs, such as channel information and max number of spatial streams.

The following NAN ASI attributes are associated with NAN operations:

- NDL attribute
- NDC attribute
- Ranging Setup attribute
- Public Availability attribute

A NAN frame that includes a NAN ASI attribute shall also include the NAN Availability attribute(s) that share the same Map ID(s) with the NAN ASI attribute.

The usages of these NAN ASI attributes are specified in the corresponding NAN operation sections:

- The usage of the Public Availability attribute is specified in section 5.2.4. The usage of the NDL attribute and NDC attribute are specified at section 6.2.3
- The usage of the Ranging Setup attribute is specified at section 8.3

Table 11 illustrates an example of NAN Availability attributes and NAN ASI attributes.

Table 11. NAN Availability attributes and NAN ASI attributes example

	Map ID	Channel	Bit Duration	Time Bitmap															
				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NAN Availability Attributes	1	36	64 TU	1				1				0				0			
		149	64 TU	0				0				1				1			
	2	6	64 TU	1				1				0				0			
		11	64 TU	0				0				0				0			
NDC Attribute	2	N/A	16 TU	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Immutable NDL Schedule	1	N/A	64 TU	0				0				1				1			

	Map ID	Channel	Bit Duration	Time Bitmap															
				16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NAN Availability Attributes	1	36	64 TU	0				0				0				0			
		149	64 TU	0				0				0				0			
	2	6	64 TU	0				0				0				0			
		11	64 TU	0				0				1				1			
NDC Attribute	2	N/A	16 TU	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Immutable NDL Schedule	1	N/A	64 TU	0				0				0				0			

	Map ID	Channel	Bit Duration	Time Bitmap															
				32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
NAN Availability Attributes	1	36	64 TU	1				1				0				0			
		149	64 TU	0				0				1				1			
	2	6	64 TU	1				1				0				0			
		11	64 TU	0				0				0				0			
NDC Attribute	2	N/A	16 TU	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Immutable NDL Schedule	1	N/A	64 TU	0				0				1				1			

	Map ID	Channel	Bit Duration	Time Bitmap															
				48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
NAN Availability Attributes	1	36	64 TU	0				0				1				1			
		149	64 TU	0				0				0				0			
	2	6	64 TU	0				0				0				0			
		11	64 TU	0				0				0				0			
NDC Attribute	2	N/A	16 TU	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Immutable NDL Schedule	1	N/A	64 TU	0				0				0				0			

5.1.2.3 Further Availability attributes

The use of the Further Availability attributes specified in this section is obsolete, and may be removed in a future release of this specification.

A NAN Device may indicate that it will be available during intervals between DWs for further service discovery or post NAN discovery operations, by including one or more of the following attributes in NAN Service Discovery frames:

- WLAN Infrastructure attribute
- P2P Operation attribute
- IBSS attribute
- Mesh attribute
- Further NAN Service Discovery attribute

If a NAN Device includes at least one of the above attributes in a NAN Service Discovery frame, it shall also include at least one Further Availability Map attribute in the same frame.

A NAN Device that includes a WLAN Infrastructure attribute in a NAN Service Discovery frame shall be in Awake state in a WLAN infrastructure network during the time intervals indicated by the values of the Map Control field and the Availability Interval Bitmap field. The available channel corresponding to each available time interval is indicated by the associated Further Availability Map attribute.

A NAN Device that includes a P2P Operation attribute in a NAN Service Discovery frame shall be in Awake state in a P2P Group or as a P2P Device during the time intervals indicated by the values of the Map Control field and the Availability Interval Bitmap field. The available channel corresponding to each available time interval is indicated by the associated Further Availability Map attribute.

A NAN Device that includes an IBSS attribute in a NAN Service Discovery frame shall be in Awake state in an IBSS network during the time intervals indicated by the values of the Map Control field and the Availability Interval Bitmap field. The available channel corresponding to each available time interval is indicated by the associated Further Availability Map attribute.

A NAN Device that includes a Mesh attribute in a NAN Service Discovery frame shall be in Awake state in a mesh network during the time intervals indicated by the values of the Map Control field and the Availability Interval Bitmap field. The available channel corresponding to each available time interval is indicated by the associated Further Availability Map attribute.

A NAN Device that includes a Further NAN Service Discovery attribute in a NAN Service Discovery frame shall be in Awake state to receive NAN Service Discovery frames during the time intervals indicated by the values of the Map Control field and the Availability Interval Bitmap field. The available channel corresponding to each available time interval is indicated by the associated Further Availability Map attribute.

More than one Further Availability Map attribute can be included in one NAN Service Discovery frame to enable a NAN Device capable of concurrent multi-band operations to indicate further availability on more than one channel for the same time intervals. Each Further Availability attribute is identified by the value of the Map ID field.

The further availability indications corresponding to a Discovery Window (Availability Intervals Bitmap bit ‘0’) in the 2.4 GHz band shall be ignored.

Whenever a NAN Device declares its availability in any of 16 TU intervals (by setting ‘1’ in the Availability Intervals Bitmap), the NAN Device shall also include at least one of the post discovery attributes or one Further NAN Service Discovery attribute and declare its availability in the corresponding interval.

Table 12 illustrates an example of the Availability Intervals Bitmap fields in a WLAN Infrastructure attribute, a P2P Operation attribute, a Further NAN Service Discovery attribute, and a Further Availability Map attribute, which are carried in a NAN Service Discovery frame received between the beginnings of two consecutive Discovery Windows.

Table 12. Further Availability Map attribute usage example

	Operating Class/ Channel Number	Availability Interval Duration	Availability Intervals Bitmap																															
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Further Availability Map Attribute	Channel 6	16 TUs	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Channel 149	16 TUs	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Channel x	16 TUs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
	Channel y	16 TUs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0
WLAN Infrastructure Attribute	–	32 TUs	0		0		0		0		0		0		0		0		1		1		1		0		0		0		0		0	
P2P Operation Attribute	–	32 TUs	0		0		0		0		0		0		0		0		0		0		0		0		1		1		1		0	
Further NAN Service Discovery Attribute	–	64 TUs	1				0				1				0				1				0				1				0			

The example indicates the following further availability information:

- The NAN Device is in Awake state in a WLAN infrastructure network from (b + 256 TUs) to (b + 352 TUs) on Channel x
- The NAN Device is in Awake state in a P2P Group or as a P2P Device from (b + 384 TUs) to (b + 480 TUs) on Channel y
- The NAN Device is in Awake state to receive NAN Service Discovery frames: 1) from (b + 16 TUs) to (b + 64 TUs) on Channel 6; 2) from (b + 128 TUs) to (b + 160 TUs) on Channel 149; 3) from (b + 256 TUs) to (b + 320 TUs) on Channel x; 4) from (b + 384 TUs) to (b + 448 TUs) on Channel y

with b representing:

- The beginning time of the DW, if the SDF containing the Further Availability Bitmap is transmitted inside the DW, or
- The beginning time of the last DW before the SDF, if the SDF containing the Further Availability Bitmap is transmitted between two consecutive DWs

A NAN Device may also include the NAN Connection Capability attribute in NAN Service Discovery frames to assist connection setup post NAN discovery.

Post NAN Discovery, whether a NAN Device establishes a connection with a peer NAN Device or not, is out the scope of this specification.

Appendix A describes an example of using Wi-Fi Direct Services to setup a P2P connection.

5.1.3 Unaligned Schedule

A NAN Device may perform non-NAN operations, such as Infrastructure connection, Bluetooth, or Wi-Fi Direct. The schedule of the non-NAN operations may not be aligned with the boundaries of NAN Slots. If a NAN Device needs to follow an unaligned schedule for non-NAN operations, it shall transmit a frame with an Unaligned Schedule attribute to indicate the corresponding unaligned schedule.

The Unaligned Schedule attribute may be carried in a unicast, multicast, or broadcast frame. More than one Unaligned Schedule attribute may be carried in a frame to indicate the NAN Device's multiple unaligned schedules. The frame that carries Unaligned Schedule attribute(s) may be any NAN management frame.

Each Unaligned Schedule attribute specifies a sequence of ULWs, which are confined by following parameters in time domain:

- Starting time of the first indicated ULW, specified by the Starting Time field
- Time duration of each ULW, specified by the Duration field
- ULW repeating interval, specified by the Period field

If the Count Down field is set to 255, the indicated ULWs does not end until next schedule update. If the Count Down field is set to zero, the NAN Device that transmits the attribute indicates the unaligned schedule ends immediately.

After a NAN Device receives the Unaligned Schedule attribute, the NAN Device uses the nearest absolute TSF timer value in past or future where the lower order 4 octets match the Start Time field as the indicated start time. If the indicated start time is in the past, then the NAN device removes the indicated ULWs time period belonging to the past from the indicated ULWs time period.

An unaligned schedule is identified by a schedule sequence ID specified by the Sequence ID field in the Unaligned Schedule attribute.

If an Unaligned Schedule attribute does not include the ULW Control field, it shall not include any band or channel information field, either. The NAN Device that transmits such an Unaligned Schedule attribute indicates that it is not available in the specified ULWs on any bands and channels. Therefore, other NAN Devices that receive such an Unaligned Schedule attribute shall not transmit any frames to the NAN Device during those ULWs. An example is shown in Figure 22.

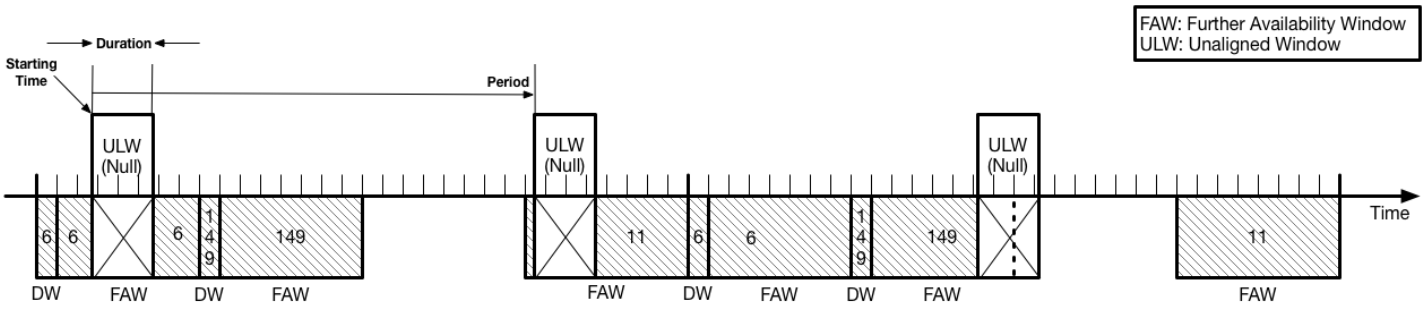


Figure 22. Unaligned Schedule attribute without Channel Information usage example

If an Unaligned Schedule attribute includes the ULW Control field, it shall also include band or channel information fields based on the values of the Type and Channel Availability subfields.

If the Channel Availability subfield is set to 0, the Unaligned Schedule attribute shall include a Band Entry field or a Channel Entry field. If a Channel Entry field is included, it may be set to specify a list of channels. The NAN Device that transmits such an Unaligned Schedule attribute indicates that it is not available only on the specified band or channels during the corresponding ULWs. Therefore, other NAN Devices that receive such an Unaligned Schedule attribute shall not transmit any frames to the NAN Device on the specified band or channels during those ULWs.

Other NAN Devices may transmit frames to the NAN Device during ULWs on a channel or band not specified in the Unaligned Schedule attribute, if the NAN Device claims it is available during the ULWs on the unspecified channel or band.

Figure 23 shows an example when a NAN Device transmits an Unaligned Schedule attribute with the Channel Availability subfield set to zero, and with a Band ID field set to 2.4 GHz band. The first two ULWs overlapped with FAWs on channels in 2.4 GHz band; therefore, the NAN Device cannot receive any frame transmissions during the ULWs. The last ULW overlaps with a FAW on Channel 149 in 5 GHz band, so the NAN Device can still receive frame transmissions during the FAW on Channel 149.

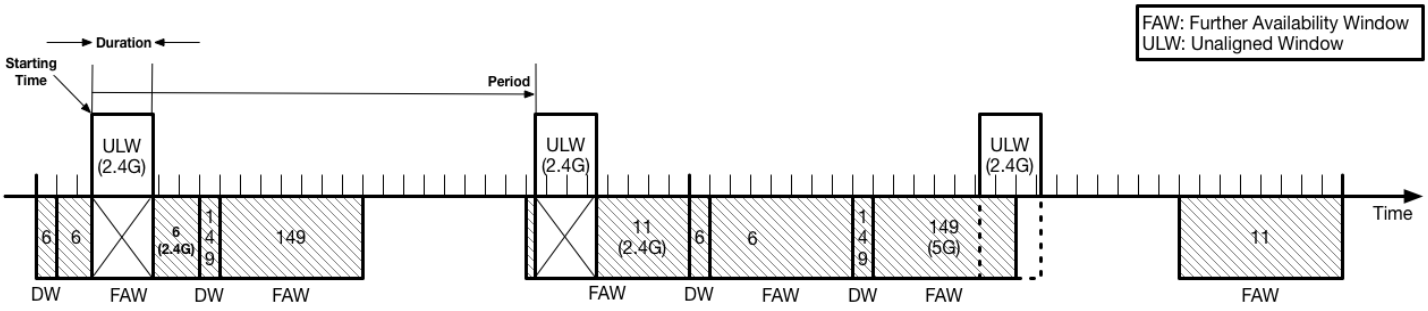


Figure 23. Unaligned Schedule attribute with Channel Availability = 0 usage example

If the Channel Availability subfield is set to one, the Unaligned Schedule attribute shall include a Channel Entry field, and the Channel Entry field shall only specify one channel. The NAN Device that transmits such an Unaligned Schedule attribute indicates that it is available on the specified channel during the corresponding ULWs. Other NAN Devices that receive the Unaligned Schedule attribute may transmit frames to the NAN Device during those ULWs on the specified channel. An example is shown in Figure 24.

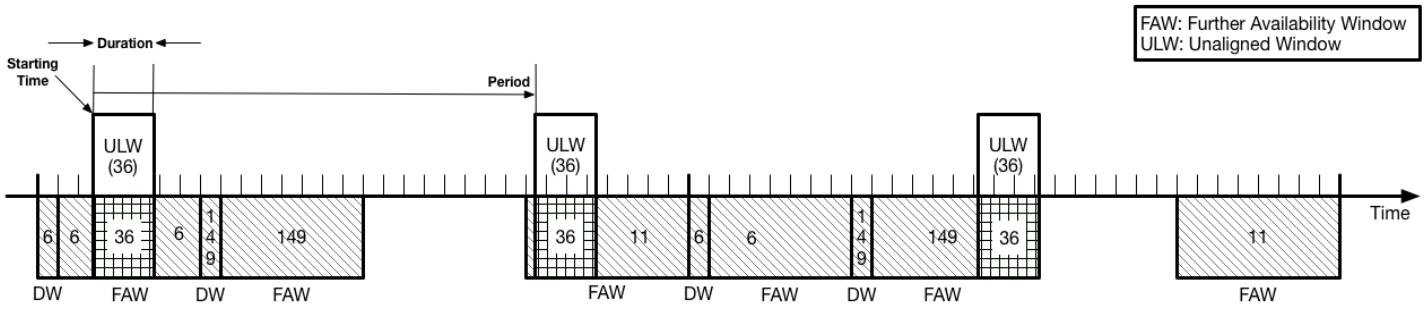


Figure 24. Unaligned Schedule attribute with Channel Availability = 1 usage example

The ULWs indicated by one or more Unaligned Schedule attributes in a same frame shall not conflict with each other. Two ULWs conflict with each other if, at the same point in time, these two ULWs

- Indicate different availability statuses; or
- Indicate availability on different primary channels

5.1.4 Sub Slot Schedule (S3)

The S3 allows a NAN Device to perform low latency Data path operations through one or more NDPs while consuming less power.

A NAN Device may indicate a refinement of the NDL CRBs with its peers using one or more S3 attributes during an NDP setup or in an NDL schedule update. An S3 attribute indicates, to a given NAN peer, the (sub) time intervals in which the device intends to be awake and present in the channel of a CRB (indicated via Committed FAW in the NAN Availability attribute).

The S3 attributes may be carried in a Data Path Setup NAF, a NDL Schedule Setup NAF, or a Schedule Update Notification NAF. The rules for updating the current S3, if any, with one or more peers are the same as those described for NAN operation schedule updates, referring to section 5.2.2 (NAN operation schedule update).

A NAN Device indicates the S3 support by setting the S3 capable bit in the Capabilities field of the Device Capability attribute. An NDP initiator should transmit an S3 attribute to an NDP responder only if the NDP responder indicates the S3 support. A NAN Device that does not support the S3 ignores a received S3 attribute, if any.

A NAN Device shall include the S3 attribute together with the Committed NAN Availability attribute present in any frame. The absence of the S3 attribute indicates that either S3 was not setup or the previously advertised S3 was terminated.

When the S3 attribute contains one or more S3 entries, each S3 entry includes the Entry Control, Time Bitmap Control, Time Bitmap Length and Time Bitmap fields, as defined in Table 114. An S3 Entry may either be applied to all NAN Availability maps or it may be applied to a single map with the Map ID specified in the Entry Control field. To facilitate NDP and NDL negotiation, the attribute also indicates whether the corresponding S3 is immutable. The Time Bitmap Control field specifies the Sub Slot duration, S3 repeat interval, and S3 start offset.

Each bit with value 1 in the Time Bitmap field indicates the device is available in the corresponding Sub Slot within a committed slot. A value of 0 indicates the device is not available in the corresponding Sub Slot.

Whenever the S3 attribute is included in any frame, the Time Bitmap in the S3 Entry field shall indicate at least one available Sub Slot within a committed slot.

Figure 25 shows an example of an S3 attribute whose format is defined in section 9.5.17.6.

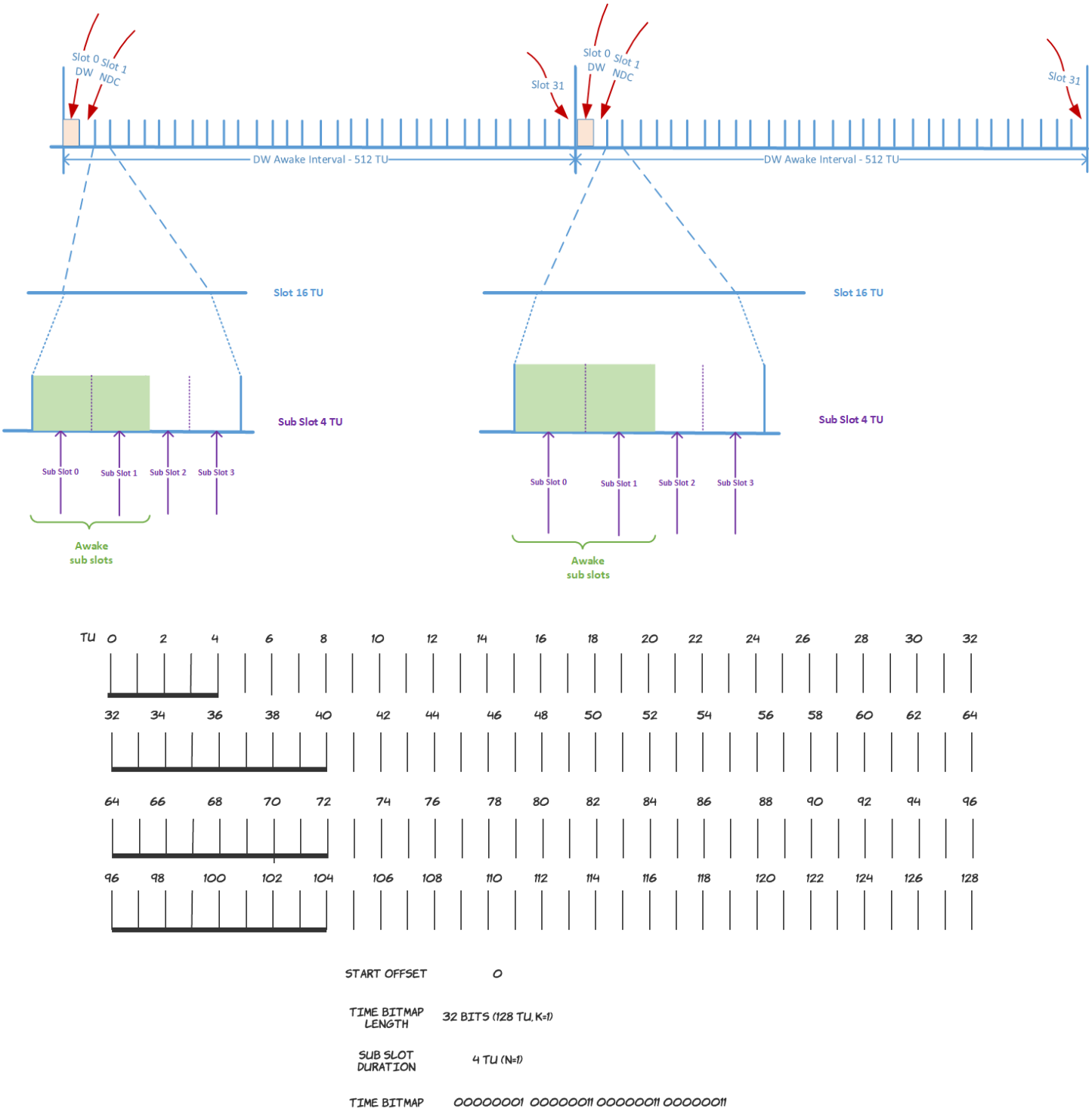


Figure 25. S3 attribute example

5.1.5 Availability Schedule precedence rules

The Committed DWs in 2.4 GHz Band shall take precedence over the Committed FAWs indicated by one NAN Availability attribute whose Map ID is specified in the 2.4 GHz DW Overwrite subfield in the Device Capability attribute. The Committed DWs in 5 GHz Band shall take precedence over the Committed FAWs indicated by either the same NAN

Availability attribute or a different one whose Map ID is specified in the 5 GHz DW Overwrite subfield in the Device Capability attribute.

The ULWs shall take precedence over all Committed DWs and all Committed FAWs if the Overwrite All flag of the ULW Overwrite field in the associated Unaligned Schedule attribute is set to one. If the Overwrite All flag is set to zero, the ULWs shall take precedence over the Committed DWs and the Committed FAWs associated with a specific NAN Availability attribute whose Map ID is specified in the Map ID subfield of the ULW Overwrite field. A usage example is shown in Figure 26.

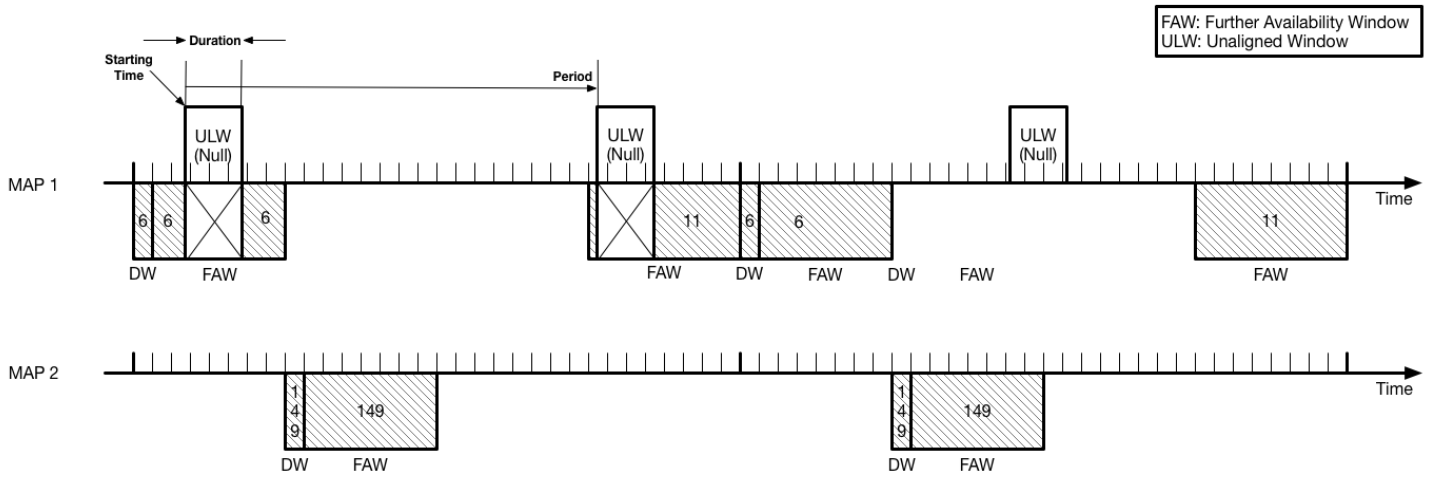


Figure 26. ULW Overwrite for a Specific NAN Availability attribute (Map 1) usage example

The schedule specified by the S3 attribute does not override any unavailable slots but refines the available and Committed slots specified by the NAN availability attribute during an NDP setup. The relative precedence of ULWs vs S3 is the same as that of ULWs vs Committed DWs and all Committed FAWs (described above).

5.1.6 FAW Overlap with DW Time

If an FAW schedule at a device overlaps with a DW that the device indicates as not present due to Power Efficient Service Discovery (section 4.2) operation, the schedule shall not use the designated discovery channel during the DW for the band indicated as available by the FAW. The discovery channels for each band are provided in section 3.2.

5.2 NAN operation schedule management

To facilitate NAN operation schedule setup and update for NAN devices that support Data Path or Ranging,

- A NAN Device that transmits a publish message or a subscribe message in a SDF shall include the Device Capability attribute in the same SDF.
- A NAN Device that transmits a publish message in a SDF shall also include at least one NAN Availability attribute with at least one Potential Availability entry or Committed Availability entry in the same SDF.
- A NAN Device that transmits a publish message in a SDF may include the Element Container attribute with the following elements in the same SDF:
  - HT Capability element
  - VHT Capability element (when VHT support is enabled)
  - HE Capability element (when HE support is enabled)

A NAN Device may use the NAN Beacon, Schedule Update Notification NAF, or any other NAN management frame to update its availability schedules, including:

- Committed DWs
- Potential and Committed FAWs
- Available and unavailable ULWs

When a NAN Device allocates FAWs for a NAN operation with a peer NAN Device, it should take into account:

1. The peer device's Potential FAWs
2. The peer device's Committed FAWs, if any
3. The peer device's S3, if any
4. Its own Potential FAWs
5. Its own Committed FAWs, if any
6. Its own S3, if any

5.2.1 NAN operation initiation scheduling

A NAN Device initiates a NAN operation by transmitting an initiation request frame, which is either a NAN Service Discovery frame (SDF) or a NAN Action frame (NAF) to a peer NAN Device, during the peer device's Committed DW or FAW, or an available ULW. The peer NAN Device shall send back an initiation response frame during the initiator's committed DW or FAW, or an available ULW. Table 13 summaries the NAN Operation Initiation frame exchanges.

Table 13. NAN Operation Initiation

NAN Operations	Initiation Request (from Initiator)	Initiation Response (from Responder)	Subsequent Initiation Messages	Post Initiation Communications	References
Further Service Discovery using Follow-up	Follow-up (SDF)	Follow-up (SDF)	None	More Follow-up frame exchanges	section 4.3
Further Service Discovery using GAS	Schedule Request (NAF)	Schedule Response (NAF)	Optionally more Schedule NAF exchanges	GAS frame exchanges	section 4.3
Ranging Setup	Ranging Request (NAF)	Ranging Response (NAF)	None	FTM frame exchanges	section 8.3
NDP Setup	Data Path Request (NAF)	Data Path Response (NAF)	Optionally more Data Path Setup NAF exchanges	Data frame exchanges	section 6.2.3

To avoid congestion in DWs and accelerate NAN operation initiation, the NAN operation initiator shall include one or more NAN Availability attributes with one or more Committed or Conditional Availability entries in the operation initiation request frame. The NAN operation responder shall include one or more NAN Availability attributes with one or more Committed or Conditional Availability entries in the operation initiation response frame, if more frame exchanges are expected. Both the initiator and the responder should make use of each other's Committed FAWs to complete the operation initiation process, and carry on post initiation communications.

NAN operations such as ranging, NDP, and further service discovery may occur in bands that are different from the band used for the NAN DWs. To ensure that the link can be closed for the NAN operation, NAN operation Initiation should be scheduled in the band that will be used for the corresponding NAN operation. The NAN operation initiator and responder should schedule Committed FAWs for the operation initiation in the band(s) intended for the respective NAN operation.

5.2.2 NAN operation schedule update

A NAN Device may use the NAN Beacon, Schedule Update Notification NAF, or any other unicast or broadcast NAN management frame to convey its updated availability schedules to one or more peer NAN Devices.

When a peer NAN Device receives a NAN management frame with updated availability schedules from the NAN Device, it shall consider the corresponding old availability schedules received from the NAN Device invalid, and shall not transmit to the NAN Device using the old availability schedules later than the second NAN Slot boundary after it receives the frame. An example of schedule update timeline is shown in Figure 27. If the received frame includes one or more NDC attributes, the peer NAN Device shall consider the old NDC schedules previously received from the NAN Device, if any, as invalid. If

the received frame does not include any NDC attribute, the peer NAN Device shall consider the NDC schedules received previously from the NAN Device, if any, are still valid.

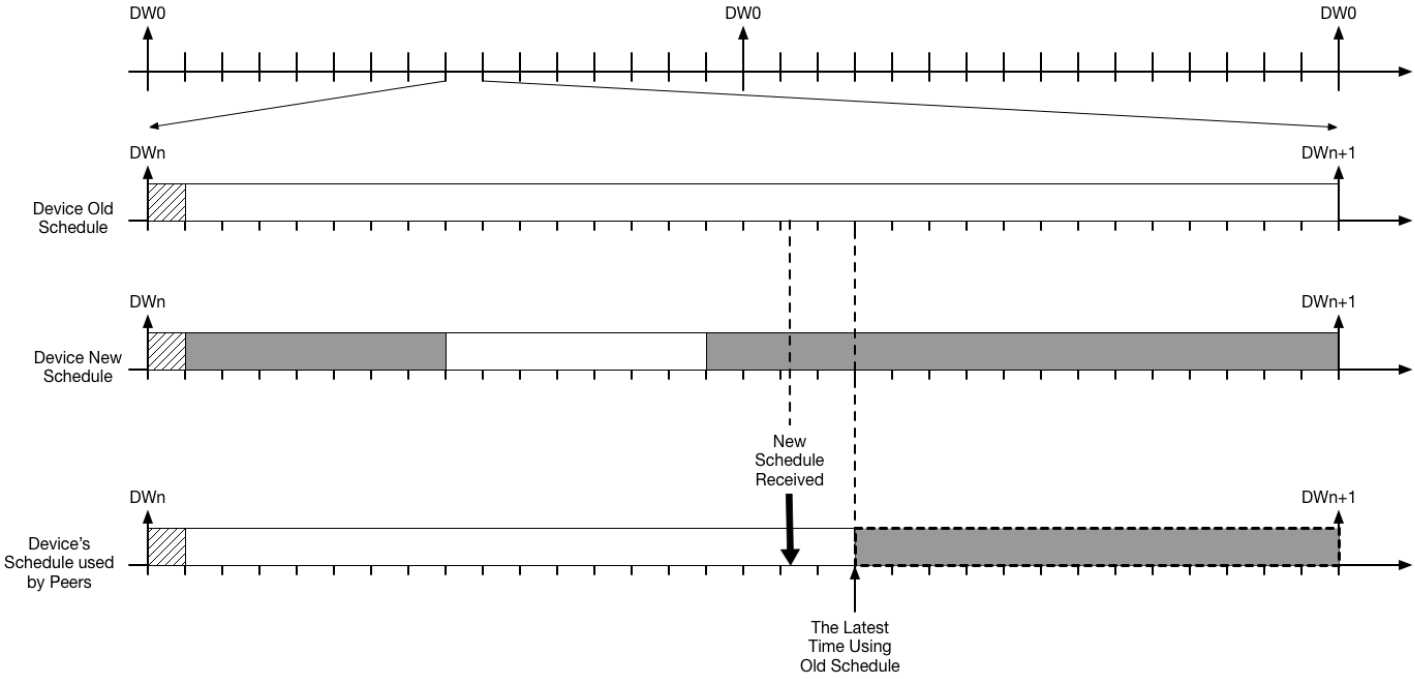


Figure 27. Schedule update timeline example

If a NAN Device needs to convey its updated availability schedules reliably to multiple peers, it may either unicast the update to each peer individually or broadcast the update to all peers multiple times. The NAN Device should use DWs or NDC CRBs to transmit broadcast schedule updates.

If the new availability schedules conflict with the old availability schedules, the NAN Device should make the new availability schedules effective at a future time point, which allows time for the NAN Device to complete the update transmissions.

To enable smooth transition from old schedules to new schedules at a future time point, the NAN Device may first convey a transition schedule as an updated schedule to all peers. The transition schedule may include a portion of the old availability schedules until the new schedule effective time, as well as a portion of the new availability schedules after the new schedule effective time. Once the new schedules become effective, the NAN Device may update all peers again with the entire new schedules.

Figure 28 shows an example of using a transition schedule to assist schedule update.

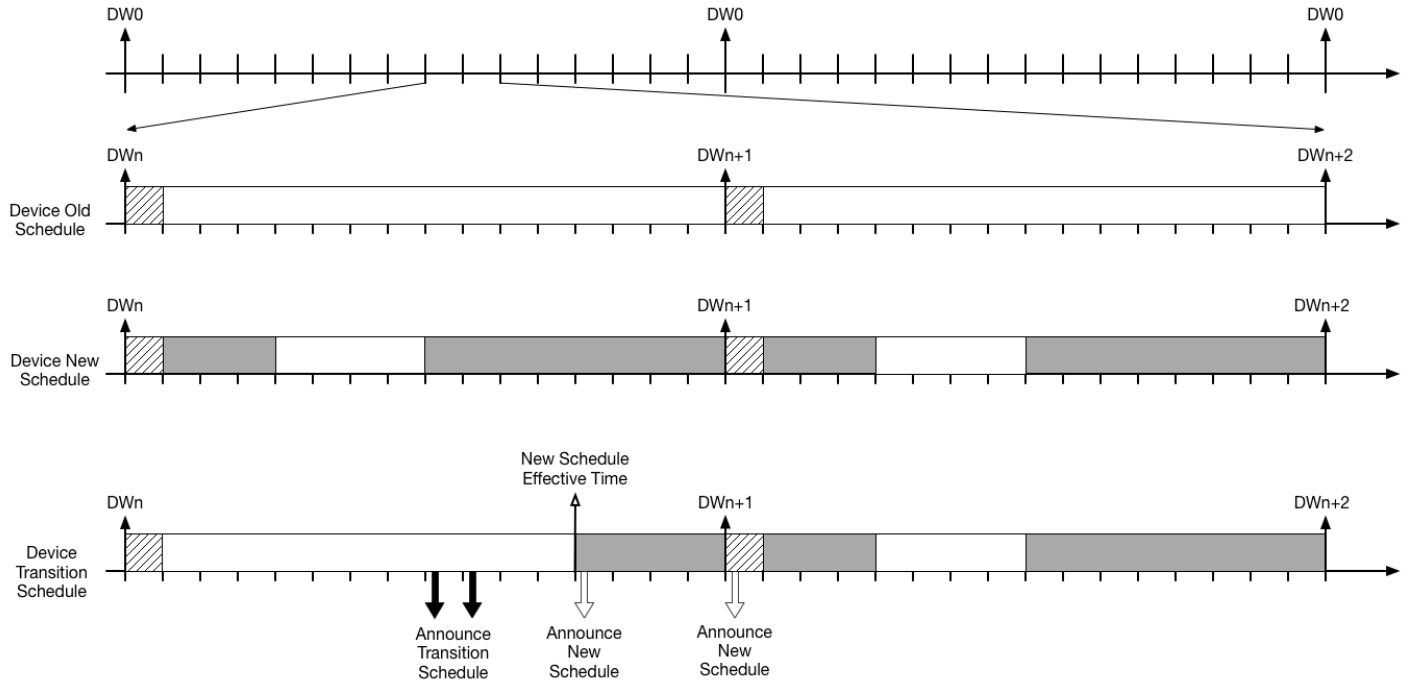


Figure 28. Transition schedule example

Since the NAN Availability attributes may only indicate a schedule starting from the previous DW0, and ending before the next DW0, a NAN Device may generate a special transition schedule as shown in Figure 29 to facilitate the transition from old schedules to new schedules effective after the next DW0.

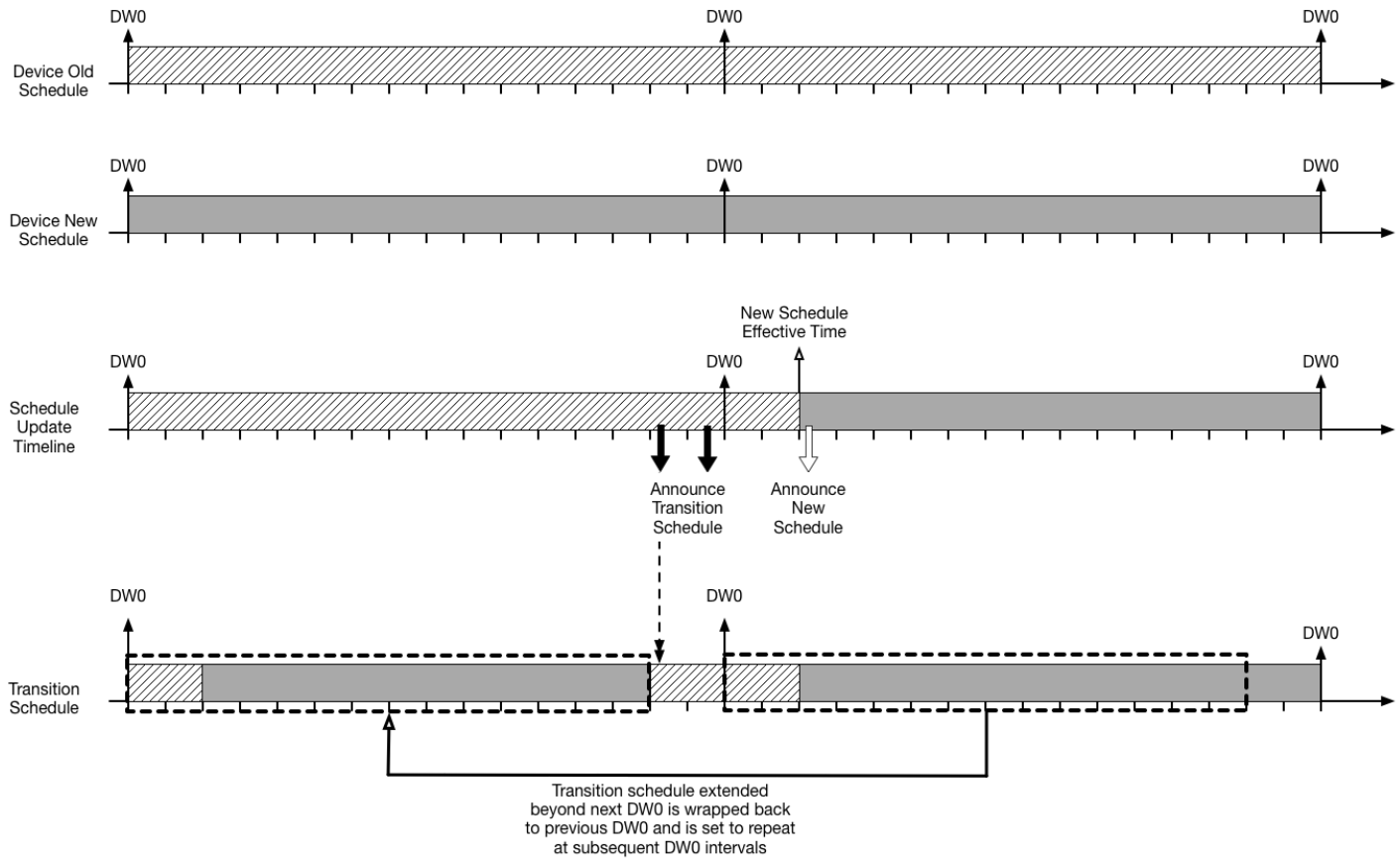


Figure 29. Transition schedule beyond DW0 boundary example

5.2.3 NAN operation in dynamic frequency selection channels

A NAN Device shall not indicate its available slots (“Potential”, “Conditional” or “Committed”) on a Dynamic Frequency Selection (DFS) channel, unless it is permitted to use the DFS channel based on regulatory requirements.

A NAN Device shall not transmit any frames to a peer NAN device on a DFS channel, unless it is permitted to use the DFS channel based on regulatory requirements.

5.2.4 Public Availability Schedule

A NAN Device may announce its Public Availability Schedule by broadcasting a NAN management frame with following attributes:

- At least one NAN Availability attribute with at least one Committed Availability entry
- The Public Availability attribute that indicates a schedule as a subset of the Committed Availability Schedule

Once a NAN Device announces its Public Availability Schedule, it shall be present during corresponding FAWs, except for those exempted by ULWs. The Public Availability Schedule shall not be canceled for power saving purpose.

The Committed Availability Schedules beyond the Public Availability Schedule may be canceled for power saving purpose. If a NAN Device broadcasts a NAN management frame that announces its Committed Availability Schedule, but without indicating the Public Availability Schedule, the whole Committed Availability Schedule shall be considered as the Public Availability Schedule, and shall not be canceled for power saving purpose.

5.3 Non-NAN operation attributes

A NAN Device capable of supporting NAN and Non-NAN concurrent operations or supporting Non-NAN operations after NAN discovery may include the corresponding Non-NAN operation attribute in NAN management frames.

Some example Non-NAN operations include:

- WLAN Infrastructure
- P2P Operation
- IBSS
- Mesh

The Non-NAN operation attributes include:

- Extended WLAN Infrastructure attribute
- Extended P2P Operation attribute
- Extended IBSS attribute
- Extended Mesh attribute

A NAN Device uses the Non-NAN operation attributes to provide some of the Non-NAN operation parameters to peer devices.

The NAN Device may generate NAN availability schedules or unaligned schedules to support the concurrent operations or Non-NAN operations after NAN discovery.

Note that the use of the following Non-NAN operation attributes is obsolete, and may be removed in a future release of this specification:

- WLAN Infrastructure attribute
- P2P Operation attribute
- IBSS attribute
- Mesh attribute

6 NAN data communication

When a service requires data path support, it instructs the NAN Device to include the Service Descriptor Extension attribute in all publish messages, with the Data Path Required flag set to one. The Data Path Type flag is set to indicate whether a NDP setup is required to support unicast data path.

The NAN Data Engine is responsible for setting up, maintaining, and tearing down NDPs. It also works with NAN Scheduler to ensure sufficient NDL CRBs are allocated to support active NDPs.

To facilitate NDP setup, a NAN Device that transmits any publish message shall include the Device Capability attribute in the same SDF that contains the publish message. A NAN Device may also include the Device Capability attribute in any other NAN management frames.

When a NAN Device receives a NAN management frame with the Device Capability attribute(s) or Element Container attribute(s) from a peer NAN Device, it shall apply the information in the received attributes immediately, and disregard the corresponding attributes received previously from the same peer NAN Device, if any.

6.1 NAN data primitives

6.1.1 Methods

6.1.1.1 Data Request method

DataRequest(type, publish_id, responder_nan_address, multicast_address, qos_requirements, security, initiator_ipv6_interface_identifier, service_specific_info)

Parameters of the DataRequest method are:

- type
  - Unicast
- publish_id
  - Identifier for the instance of the Publisher function associated with the data path setup request
- responder_nan_address
  - The Responder’s NAN NMI
- multicast_address (reserved for multicast)
  - The MAC address that is set to the A1 field of multicast frames
- qos_requirements (for unicast only)
  - Unicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [3], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- qos_requirements (reserved for multicast)
  - Multicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included

  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included

- security
  - Open Security
  - Need Security

    - CSID

    - ND-PMKID and ND-PMK for NCS-SK cipher suites

  - Identifies additional frame protection required

    - Group addressed data frame protection

    - Group addressed management frame protection

- initiator_ipv6_interface_identifier (optional)
  - The NDP Initiator's IPv6 Link Local Interface Identifier
- service_specific_Info
  - Sequence of values which are to be transmitted in the frame body

The DataRequest method returns

For Unicast

- ndp_id
  - A non-zero value that is assigned by the NAN Data Engine for the NDP and which uniquely identifies the NDP instance of this device
- initiator_data_address
  - The NDP Initiator's data interface address for the NDP

6.1.1.2 Data Response method

DataResponse(type, status, ndp_id or mc_id, initiator_data_address, multicast_address, qos_requirements, security, responder_ipv6_interface_identifier, service_specific_info)

Parameters of the DataResponse method are:

- type
  - unicast
- status
  - Decision (Accepted/Rejected)
  - Reason Code
- ndp_id (for unicast only)
  - Identifier for the instance of the NDP
- mc_id (reserved for multicast)
  - Identifier for the multicast enroll instance at the enrollee.
- initiator_data_address (for unicast only)
  - The NDP Initiator's data interface address for the NDP
- multicast_address (reserved for multicast)
  - The MAC address that is set to the A1 field of multicast frames

- qos_requirements (for unicast only)
  - Unicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- qos_requirements (reserved for multicast)
  - Multicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- security
  - Open Security
  - Need Security

    - CSID

    - ND-PMKID and ND-PMK for NCS-SK cipher suites

  - Identifies additional frame protection required

    - Group addressed data frame protection

    - Group addressed management frame protection
- responder_ipv6_interface_identifier (optional)
  - The NDP Responder’s IPv6 Link Local Interface Identifier
- service_specific_Info
  - Sequence of values which are to be transmitted in the frame body

6.1.1.3 Data End method

DataEnd(type, status, ndp_id, nmsg_id, initiator_data_address)

Parameters of the DataEnd method are:

- type
  - Unicast
- Status
  - Reason Code
- ndp_id (for unicast only)
  - Identifier for the instance of the NDP
- nmsg_id (reserved for multicast)
  - NAN Multicast Service Group ID
- initiator_data_address (for unicast only)

- The NDP Initiator’s data interface address for the NDP

6.1.1.4 Data Update method

DataUpdate(type, ndp_id, nmsg_id, initiator_data_address, qos_requirements)

Parameters of the DataUpdate method are:

- type
  - Unicast
- ndp_id (for unicast only)
  - Identifier for the instance of the NDP
- nmsg_id (reserved for multicast)
  - NAN Multicast Service Group ID
- initiator_data_address (for unicast only)
  - The NDP Initiator’s data interface address for the NDP
- qos_requirements (for unicast only)
  - Unicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included
- qos_requirements (reserved for multicast)
  - Multicast Traffic identifier (TID): an identifier usable by higher layer entities to distinguish data packet to MAC entities, as defined in [1], if available. Otherwise, not included
  - Service data packet size: contains an unsigned integer that specifies the size of service data packets belonging to the stream, if available. Otherwise, not included
  - Mean Data Rate: indicates the average data rate specified at the MAC for transport of packets belonging to the stream, if available. Otherwise, not included
  - Maximum Service Interval: specifies the latency limit allowed to transport a data packet belonging to the stream, if available. Otherwise, not included

6.1.2 Events

6.1.2.1 Data Indication event

DataIndication(type, publish_id, ndp_id or mc_id, initiator_data_address, responder_data_address, security, initiator_ipv6_interface_identifier, service_specific_info)

Parameters of the DataIndication event are:

- type
  - Unicast
- publish_id
  - Identifier for the instance of the Publisher function associated with the data path setup request
- ndp_id (for unicast only)

  - A non-zero value that is assigned by the NAN Data Engine for the NDP and which uniquely identifies the NDP instance of this device
- mc_id (reserved for multicast)
  - Identifier for the multicast enroll instance at the enrollee
- initiator_data_address (for unicast only)
  - The NDP Initiator's data interface address for the NDP
- responder_data_address (for unicast only)
  - The NDP Responder's data interface address for the NDP
- security
  - Open Security
  - Need Security

    - CSID

    - ND-PMKID for NCS-SK cipher suites
- initiator_ipv6_interface_identifier (optional)
  - The NDP Initiator's IPv6 Link Local Interface Identifier
- service_specific_Info
  - Sequence of values which were decoded from the received frame

6.1.2.2 Data Confirm event

DataConfirm(type, status, ndp_id or mc_id, nmsg_id, initiator_data_address, responder_data_address, responder_ipv6_interface_identifier, service_specific_specific_info)

Parameters of the DataConfirm event are:

- type
  - Unicast
- Status
  - Decision (Accepted/Rejected)
  - Reason Code
- ndp_id (for unicast only)
  - Identifier for the instance of the NDP
- mc_id (reserved for multicast only)
  - Identifier for the multicast enroll instance at the enrollee
- nmsg_id (reserved for multicast)
  - NAN Multicast Service Group ID
- initiator_data_address (for unicast only)
  - The NDP Initiator's data interface address for the NDP
- responder_data_address (for unicast only)
  - The NDP Responder's data interface address for the NDP
- responder_ipv6_interface_identifier (optional)
  - The NDP Responder's IPv6 Link Local Interface Identifier

- service_specific_Info
  - Sequence of values which were decoded from the received frame

6.1.2.3 Data Termination event

DataTermination(type, status, ndp_id or mc_id, nmsg_id, initiator_data_address)

Parameters of the DataTermination event are:

- type
  - Unicast
- Status
  - Reason Code
- ndp_id (for unicast only)
  - Identifier for the instance of the NDP
- mc_id (reserved for multicast)
  - Identifier for the multicast enroll instance at the enrollee
- nmsg_id (reserved for multicast)
  - NAN Multicast Service Group ID
- initiator_data_address (for unicast only)
  - The NDP Initiator's data interface address for the NDP

6.2 Unicast operation

A service subscriber initiates a NDP setup for a service instance and serves as an NDP Initiator upon receiving a DataRequest method call with the Type set to "Unicast". The intended service publisher serves as the NDP Responder.

The NDP Initiator shall start the NDP setup together with the NDL Schedule setup,

- If there is not yet an existing NDL Schedule established between the NDP Initiator and the NDP Responder; or
- There is already an existing NDL Schedule established between the NDP Initiator and the NDP Responder, but it does not meet the requirements of the new NDP

The NDP Initiator may start the NDP setup without the NDL Schedule setup if there is already an existing NDL schedule established between the NDP Initiator and the NDP Responder, and the existing NDL schedule meets the requirements of the new NDP.

The NDP Initiator shall start the NDP setup together with a ND-TKSA if:

- The Security parameter in the DataRequest method call is set to "Need Security", and
- The existing ND-TKSAs between the NDP Initiator and the NDP Responder, if any, do not meet the security requirements of the new NDP

Otherwise, the NDP Initiator shall start the NDP setup without a new Pairwise Security Association.

6.2.1 NDP setup without ND-TKSA

The NDP Initiator starts the NDP setup by

- Generating a ndp_id
- Selecting a NDI for the new NDP
- Transmitting a Data Path Request NAF to the intended NDP Responder

The Data Path Request NAF shall include

- The NDP/NDPE attribute with the Type subfield set to “Request”
- The Device Capability attribute
- The Element Container attribute with the following elements (section 0)
  - HT Capability element
  - VHT Capability element (when VHT support is enabled)
  - HE Capability element (when HE support is enabled)

When the NDP Responder receives the Data Path Request NAF with the “Request” NDP/NDPE attribute, it generates a DataIndication event with the type set to Unicast to report the NDP setup request from the NDP Initiator.

Once the NDP Responder receives the DataResponse method call associated with the NDP setup request, and the Status parameter is set to “Rejected”, the NDP Responder shall terminate the NDP setup and transmit a Data Path Response NAF to the NDP Initiator. The Data Path Response NAF shall include the NDP/NDPE attribute with the Type subfield set to “Response” and the Status subfield set to “Rejected”.

If the NDP Responder receives the DataResponse method call associated with the NDP setup request, and the Status parameter of the DataResponse method call is set to “Accepted”, it consults the NAN Scheduler to check whether a NDL Schedule has been established with the NDP Initiator to accommodate the new NDP. Based on the feedback from the NAN Scheduler, the NDP Responder decides to either accept or reject the NDP setup request.

If the NDP Responder decides to reject the NDP setup request, it shall transmit a Data Path Response NAF to the NDP Initiator, which includes the NDP/NDPE attribute with the Type subfield set to “Response” and the Status subfield set to “Rejected”.

If the NDP Responder decides to accept the NDP setup request, it shall select a NDI for the NDP, and transmit a Data Path Response NAF to the NDP Initiator. The Data Path Response NAF shall include:

- The NDP/NDPE attribute with the Type subfield set to “Response” and the Status subfield set to “Accepted”
- The Device Capability attribute
- The Element Container attribute with the following elements (section 0)
  - HT Capability element
  - VHT Capability element (when VHT support is enabled)
  - HE Capability element (when HE support is enabled)

After the NDP Responder transmits the Data Path Response NAF to the NDP Initiator,

- If the NDP setup is started without the NDL Schedule setup, it generates a DataConfirm event to report the result of the NDP setup process
- If the NDP setup is started together with the NDL Schedule setup, the operation is specified in section 6.2.3.3

When the NDP Initiator receives the NDP attribute/NDPE with the Type subfield set to "Response" and the Status subfield set to “Rejected” in the Data Path Response NAF, it terminates the NDP setup and generates a DataConfirm event with the status set to “Rejected” and also with a Reason Code.

When the NDP Initiator receives the NDP/NDPE attribute with the Type subfield set to "Response" and the Status subfield set to “Accepted” in the Data Path Response NAF,

- If the NDP setup is started without the NDL Schedule setup, it completes the NDP setup and generates a DataConfirm event with the status set to “Accepted”
- If the NDP setup is started together with the NDL Schedule setup, the operation is specified in section 6.2.3.3

Figure 30 shows the NDP setup protocol without ND-TKSA and NDL Schedule setup.

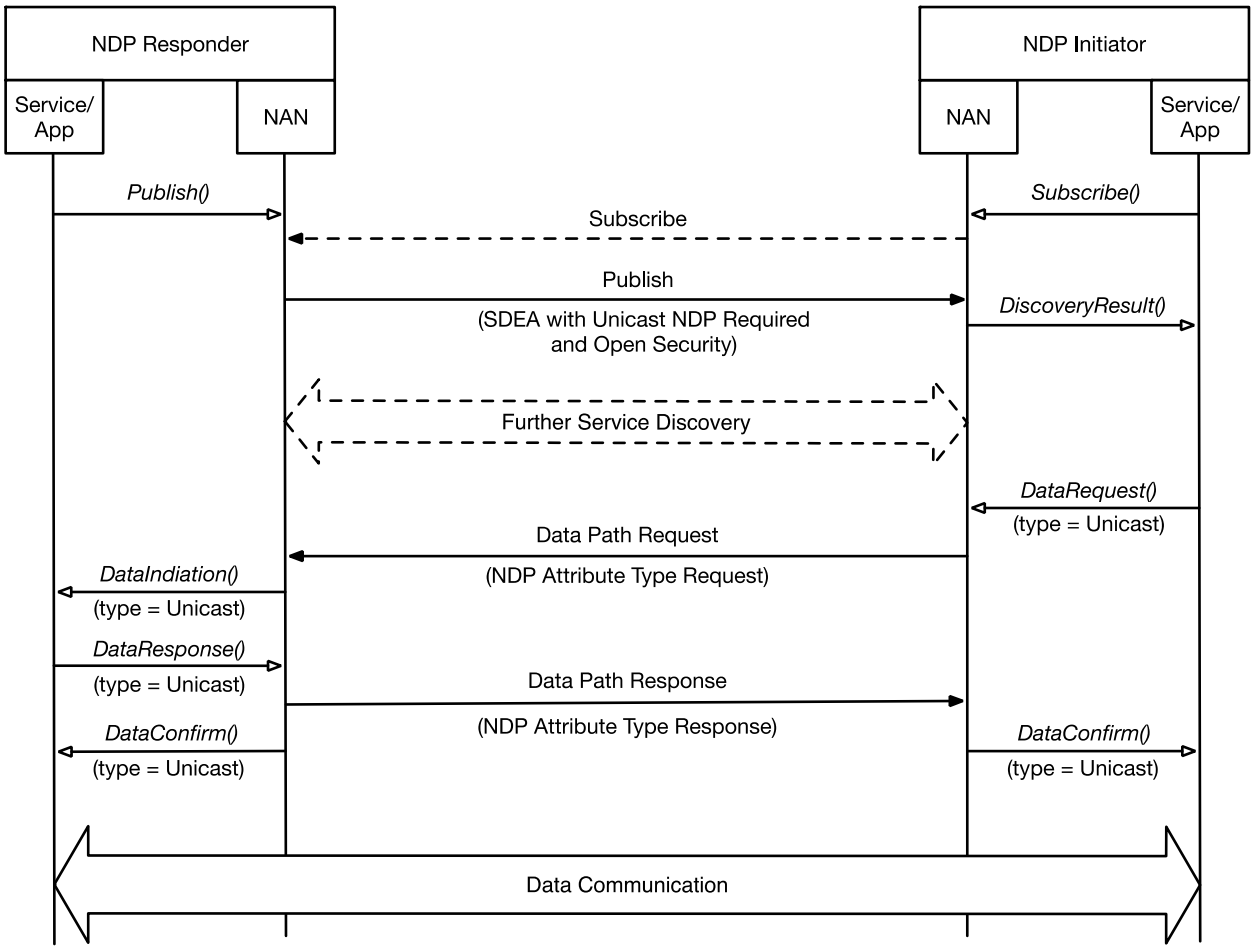


Figure 30. NDP setup without ND-TKSA and NDL schedule setup

6.2.2 NDP setup with ND-TKSA

If the NDP Initiator starts the NDP setup together with a ND-TKSA, the setup protocol is a 4-way handshake, as show in Figure 31.

In addition to the NDP/NDPE attribute and other attributes required for the NDP setup, the Data Path Setup NAFs shall also include security attributes, as specified in section 7.1.3.1.

The NDP Initiator and the NDP Responder generate the DataConfirm event with the status set to “Accepted” when both the NDP setup and the ND-TKSA are completed successfully; otherwise, the DataConfirm event is generated with the status set to “Rejected” and also one of the Reason Codes listed in Table 43.

The NDP setup with both the ND-TKSA and the NDL Schedule setup is specified in section 6.2.3.3.

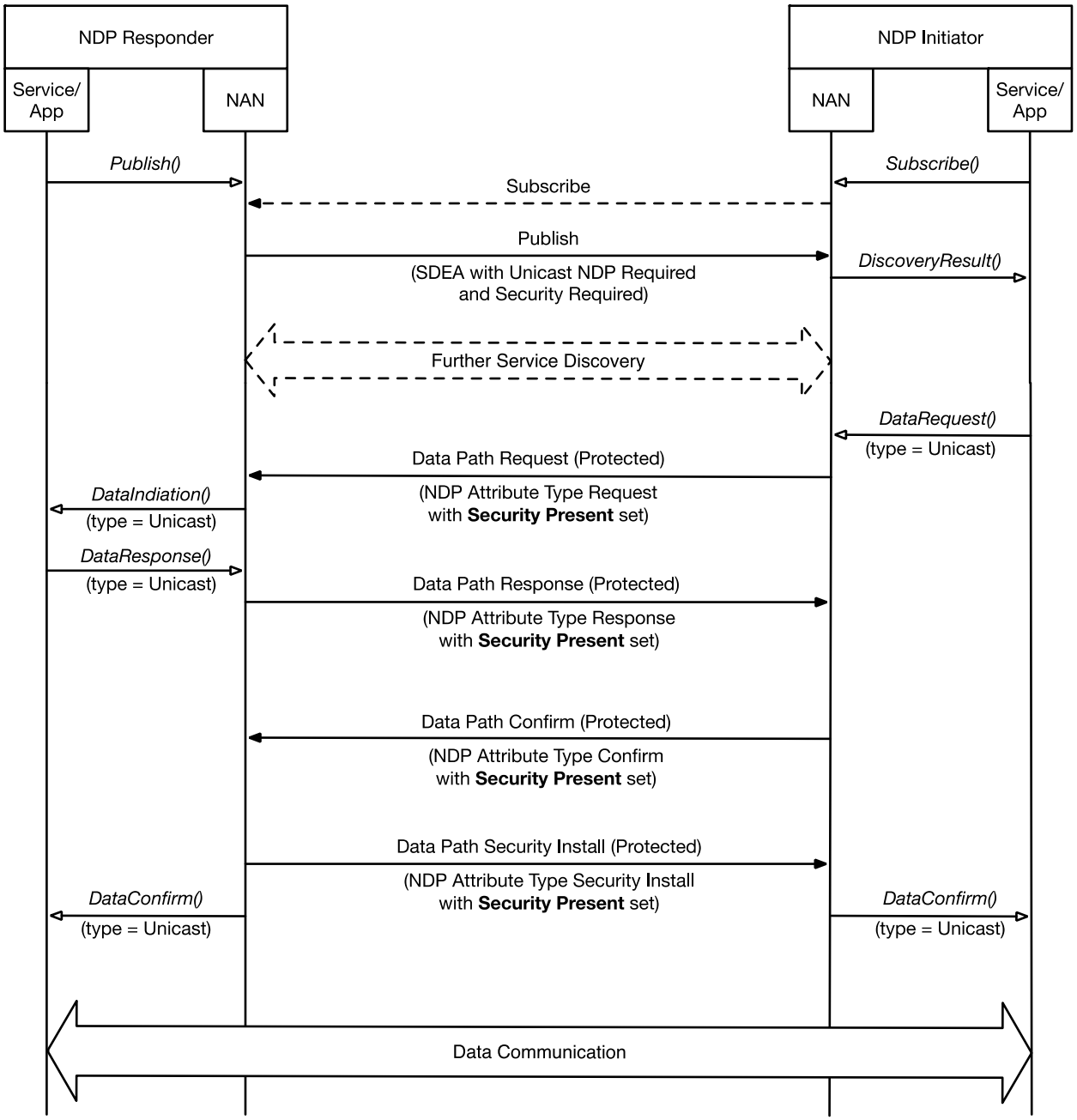


Figure 31. NDP setup with ND-TKSA and without NDL schedule setup

6.2.3 NDL Schedule setup

6.2.3.1 NDL Schedule

When a NDP Initiator sets up a new NDP with a NDP Responder, the NDP Initiator shall also establish a NDL Schedule with the NDP Responder if there is not yet an existing NDL Schedule between the two NAN Devices.

A NDL Schedule is uniquely identified by the NMIs of the two NAN Devices that establish the NDL.

Two NAN Devices establish a NDL Schedule by exchanging their Potential, Conditional, and Committed FAWs, as specified in section 6.2.3.3 and 6.2.3.4. The NDL Schedule, once established, consists of one or more NDL CRBs, which are essentially the overlapped portions of the two NAN Devices' Committed FAWs with the same primary channel. The two NAN Devices should ensure the NDL Schedule include sufficient NDL CRBs to support the new NDP.

Once two NAN Devices establish a NDL, they may update the NDL Schedule, if needed, to:

- Accommodate newly established NDPs
- Fulfill new data communication requirements from existing NDPs
- Adapt to availability schedule changes on either NAN Device

6.2.3.2 NDC Schedule

When two NAN Devices establish a new NDL, and decide not to enroll the new NDL into any existing NDC, the new NDL starts a new NDC. The two NAN Devices that create the first NDL of a NDC shall decide the NDC ID and the initial NDC Schedule, as specified in section 6.2.3.3. The initial NDC Schedule shall be a subset of the first NDL's schedule.

When two NAN Devices establish a new NDL, and decide to enroll the new NDL into an existing NDC, they shall ensure the NDL Schedule is a superset of the existing NDC's Base Schedule.

The NDC Schedule consists of one or more NDC CRBs.

Figure 32 shows an example of NDL CRBs and NDC CRBs.

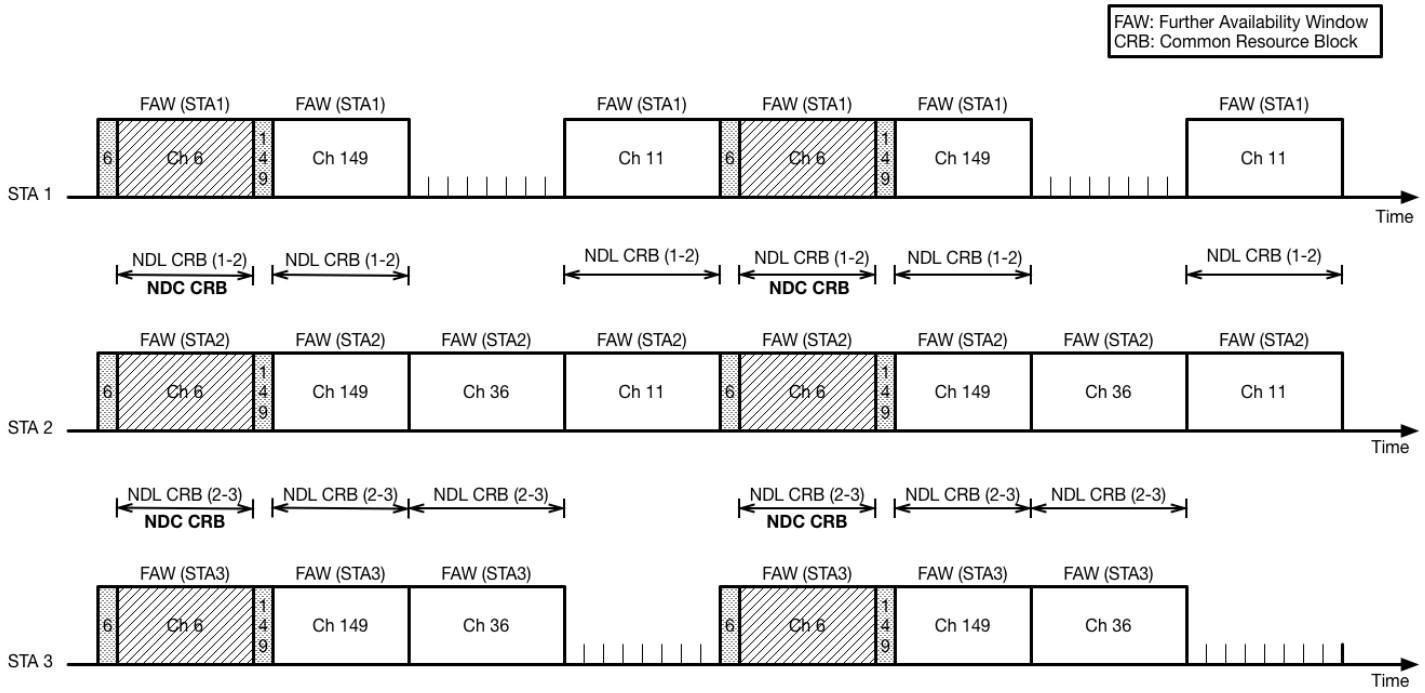


Figure 32. NDL CRB and NDC CRB example

A NAN Device may participate in a single NDC at one time, or it may participate in multiple NDCs concurrently.

If a NAN Device participates in one or more NDCs, and it transmits a publish message in a SDF, it should include the corresponding NDC attributes in the same SDF.

6.2.3.3 NDL Schedule setup together with NDP setup

When a NDP Initiator starts the NDP setup together with the NDL Schedule setup, it serves as the NDL Initiator, and the NDP Responder serves as the NDL Responder.

In addition to the NDP/NDPE attribute and other attributes required for the NDP setup, the NDP/NDL Initiator and the NDP/NDL Responder shall also include the NDL attribute and the NDL Schedule proposals in the Data Path Setup NAFs, as specified below.

The NDP/NDL Initiator should first select an NDC for the NDL and propose it during the NDL Schedule setup.

To select an NDC, the NDP/NDL Initiator may create a new NDC, or select one of the NDCs it participates in, or select one of the NDCs that the NDP/NDL Responder advertises in its transmitted NDC attributes, if any.

If the NDP/NDL Initiator decides to create a new NDC for the NDL, it shall generate the NDC ID and select the NDC Schedule for the new NDC. The NDP/NDL Initiator is recommended to select the default NDC Schedules, as specified in Table 14, for the new NDC, unless it has any schedule constraint that conflicts with the default NDC Schedules.

Table 14. Default NDC Schedule

	For communication with 2.4GHz only NAN Device	For communication with 2.4/5GHz dual-band NAN Device
Time Window	One NAN Slot immediately following each committed 2.4 GHz DW	One NAN Slot immediately following each committed 5 GHz DW
Channel	6	149 or 44

If the NDP/NDL Initiator chooses to join an existing NDC that it participates in, it shall use the NDC Schedule of the chosen NDC.

The NDP/NDL Initiator may choose not to propose a NDC for the NDL, and thus make the NDP/NDL Responder select the NDC.

The NDP/NDL Initiator may also propose an Immutable NDL Schedule and specify the QoS Requirements for the NDL.

NDP and NDL Schedule Setup without NDP Confirm Required

The NDP/NDL Initiator starts the NDP and NDL Schedule setup by transmitting a Data Path Request NAF to the NDP/NDL Responder. This section explains the behavior when the NDP/NDL Initiator unsets the “Confirm Required” flag in the “Request” NDP/NDPE attribute in the Data Path Request NAF.

The Data Path Request NAF shall include a NDL attribute with the Type subfield set to “Request”, and shall also include a NDL Schedule Initial Proposal:

- The NDL Schedule Initial Proposal shall include one or more NAN Availability attributes with one or more Committed or Conditional Availability entries, which shall indicate Conditional or Committed FAWs that contain:
  - The NDC CRBs indicated by the proposed NDC, if the NDL Schedule Initial Proposal includes a NDC attribute with the Selected NDC flag in the Schedule Control field set to one
  - The NDL CRBs indicated by the Immutable NDL Schedule, if the NDL attribute Type subfield is set to "Request" and includes the Immutable Schedule field to indicate the strongly suggested NDL CRBs for the NDL Schedule
  - Sufficient NDL CRBs that fulfill the QoS requirements indicated by the NDL QoS attribute, if included in the NDL Schedule Initial Proposal
- The included NAN Availability attributes should also include one or more Potential Availability entries (if the NDP/NDL Initiator does not provide any Potential Availability entry, the NDP/NDL Responder has limited options to counter the NDL Schedule Initial Proposal)
- The NDL Schedule Initial Proposal may also include one or more NDC attributes, which indicate the existing NDCs that the NDP/NDL Initiator is participating in

The Data Path Request NAF with a NDL Schedule Initial Proposal may also include one or more S3 attributes.

In response to the received Data Path Request NAF with the NDL attribute Type subfield is set to "Request" and a NDL Schedule Initial Proposal, the NDP/NDL Responder shall send back a Data Path Response NAF with a NDL attribute, and shall set the Type subfield of the NDL attribute to “Response”:

- If the NDP/NDL Responder rejects the NDP setup request with a reason code set to “NDP_REJECTED”, it shall set the Status subfield of the NDL attribute to “Rejected” with a reason code also set to “NDP_REJECTED”
- If the NDP/NDL Responder rejects the NDL setup request for any reason other than “NDP_REJECTED”, it shall set the Status subfield of the NDP/NDPE attribute to “Rejected” with a reason code set to “NDL_UNACCEPTABLE”
- If the NDP/NDL Responder accepts the NDP setup request, it may either accept or counter the NDL Schedule Initial Proposal by setting the Status subfield of the NDL attribute to “Accepted” or “Continued”

Table 15 summarizes the relationship between the Status values in the NDP/NDPE attribute and the NDL attribute included in the Data Path Response NAF.

Table 15. Relationship between NDP Status and NDL Status in Data Path Response NAF without NDP Confirm

NDP Status	NDL Status		
	Accepted	Continued	Rejected
Accepted	Allowed	Allowed	Not Allowed
Rejected	Not Allowed	Not Allowed	Allowed

If the received NDL Schedule Initial Proposal has invalid availability indication such as invalid NAN availability with overlapping time slots with different channels, NDC outside NAN availability, or Immutable outside NAN availability, the NDP/NDL responder shall reject the NDL Schedule Initial Proposal by setting the Status subfield of the NDL attribute to "Rejected" with a reason code set to "INVALID AVAILABILITY".

If the received NDL Schedule Initial Proposal contains any Immutable NDL Schedule, including any immutable S3, the NDP/NDL Responder may:

- Accept the proposal and include the Immutable NDL Schedule in its Committed FAWs; or
- Counter the proposal by accepting the Immutable NDL Schedule and proposing additional NDL CRBs not included in the NDL Schedule Initial Proposal; or
- Reject the proposal with the reason code set to "IMMUTABLE_UNACCEPTABLE"

If the received NDL Schedule Initial Proposal contains the NDL QoS attribute, the NDP/NDL Responder may:

- Accept or counter the proposal, and shall fulfill the QoS requirements specified by the NDL QoS attribute; or
- Reject the proposal with the reason code set to "QoS_UNACCEPTABLE"

If the NDP/NDL responder accepts the proposed immutable NDL Schedule, then the preferred primary channel of the NDP/NDL responder for the time slots in the accepted immutable NDL schedule shall be the same as the indicated preferred primary channel of the peer device for the proposed immutable NDL Schedule.

NOTE: If the NDP/NDL Responder cannot accept the Immutable NDL Schedule or cannot fulfill the QoS requirements from the NDL Schedule Initial Proposal, it can only reject the proposal.

If the received NDL Schedule Initial Proposal contains a proposed NDC, the NDP/NDL Responder may accept the proposed NDC, or reject the proposed NDC, or counter the proposed NDC by selecting a different NDC for the NDL.

If the NDP/NDL responder accepts the proposed NDC, then the preferred primary channel of the NDP/NDL responder for the time slots in the accepted NDC shall be the same as the indicated preferred primary channel of the peer device for the proposed NDC.

To select a NDC, the NDP/NDL Responder may create a new NDC, or pick one of the NDCs it participates in, or pick one of the NDCs the NDP/NDL Initiator participates in, if any. If the NDP/NDL Responder decides to create a new NDC for the NDL, it shall generate the NDC ID and select the NDC Schedule for the new NDC. The NDP/NDL Responder is recommended to select the default NDC Schedules, as specified in Table 14, for the new NDC, unless it has any schedule constraint that conflicts with the default NDC Schedules.

If the NDP/NDL Responder chooses an existing NDC it participates in, it shall use the NDC Schedule of the chosen NDC. If the received NDL Schedule Initial Proposal does not contain a proposed NDC, the NDP/NDL Responder may assume any subset of the NDL Schedule Initial Proposal is acceptable as the NDC schedule for the NDP/NDL Initiator.

If the NDP/NDL Responder sets the Status subfield of the "Response" NDL attribute to "Accepted" in the Data Path Response NAF, the NAF shall also include a NDL Schedule Compliant Proposal (refer to Table 16).

- The NDL Schedule Compliant Proposal shall include one or more NAN Availability attributes with one or more Committed Availability entries, which shall indicate Committed FAWs that at least contain:

  - The NDC CRBs indicated by the proposed NDC in the NDL Schedule Initial Proposal (if any); or a subset of the NDL Schedule Initial Proposal as the NDC CRBs (if there is not a proposed NDC in the NDL Schedule Initial Proposal)
  - The NDL CRBs indicated by the Immutable NDL Schedule, if included in the NDL Schedule Initial Proposal
  - Sufficient NDL CRBs that fulfill the QoS requirements indicated by the NDL QoS attribute, if included in the NDL Schedule Initial Proposal
- The NDL Schedule Compliant Proposal shall also include the NDC attribute with the Selected NDC flag set to one, which indicates the agreed NDC for the NDL

NOTE: The NDL Schedule Compliant Proposal may also contain additional Committed FAWs either included or not included in the NDL Schedule Initial Proposal.

Table 16. Key components in NAN Schedule Initial and Compliant Proposals

NAN Schedule Initial Proposal in Data Path Request				**NAN Schedule Compliant Proposal in Data Path Response (NDL status = Accepted)**	
A. Conditional or Committed FAWs indicated by NAN Availability attributes	**B. Immutable NDL CRBs indicated by Immutable schedules in NDL attribute**	**C. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**Q. QoS Requirements indicated by NDL QoS attribute**	**D. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**E. Committed FAWs indicated by NAN Availability attributes**
Yes (included)	No	No	No	Subset of A	Superset of D
Yes	Yes (subset of A)	No	No	Subset of A	Superset of B and D
Yes	No	Yes (subset of A)	No	Same as C	Superset of D
Yes	Yes (subset of A)	Yes (subset of A)	No	Same as C	Superset of B and D
Yes	No	No	Yes	Subset of A	Superset of D and Q
Yes	Yes (subset of A)	No	Yes	Subset of A	Superset of B, D, and Q
Yes	No	Yes (subset of A)	Yes	Same as C	Superset of D and Q
Yes	Yes (subset of A)	Yes (subset of A)	Yes	Same as C	Superset of B, D, and Q

After the NDP/NDL Responder transmits the Data Path Response NAF with the "Response" NDL attribute and the NDL Schedule Compliant Proposal, it completes its NDL Schedule setup and shall be present during its Committed FAWs, indicated by the NDL Schedule Compliant Proposal.

If the NDP/NDL Responder transmits the “Response” NDL attribute with the Status subfield set to “Rejected” in the Data Path Response NAF, it terminates its NDP set up and the NDL Schedule setup.

The “Response” NDL attribute shall include a valid reason code. The Data Path Response NAF may also include the NDL Schedule Suggested Proposal that includes the following attributes:

- A NDC attribute with the Selected NDC flag in the Schedule Control field set to one, which indicates the proposed NDC for the NDL
- One or more NAN Availability attributes with one or more Committed or Potential Availability entries

Note that the NDC and NDL CRBs indicated by the NDL Schedule Suggested Proposal need not be overlapped with those indicated by the NDL Schedule Initial Proposal.

The Data Path Response NAF with a NDL Schedule Suggested Proposal may also include one or more S3 attributes.

If the NDP/NDL Responder sets the Status subfield of the “Response” NDL attribute to “Continued” in the Data Path Response NAF, the NAF shall also include a NDL Schedule Counter Proposal (refer to Table 17).

The NDL Schedule Counter Proposal shall include the following attributes:

- A NDC attribute with the Selected NDC flag in the Schedule Control field set to one, which indicates the proposed NDC for the NDL
- One or more NAN Availability attributes with one or more Committed or Conditional Availability entries, which shall indicate Conditional or Committed FAWs that contain:
  - The NDC CRBs indicated by the proposed NDC in the NDL Schedule Counter Proposal
  - The NDL CRBs indicated by the Immutable NDL Schedule in the “Request” NDL attribute, if any
  - Sufficient NDL CRBs that fulfill the QoS requirements indicated by the NDL QoS attribute, if included in the NDL Schedule Initial Proposal
  - The NDL CRBs indicated by the Immutable NDL Schedule in the “Response” NDL attribute, if any
  - Sufficient NDL CRBs that fulfill the QoS requirements indicated by the NDL QoS attribute, if included in the NDL Schedule Counter Proposal

The Data Path Response NAF with a NDL Schedule Counter Proposal may also include one or more S3 attributes.

The NDC CRBs indicated by the proposed NDC in the NDL Schedule Counter Proposal need not be overlapped with those indicated by the proposed NDC in the NDL Schedule Initial Proposal. The NDL CRBs indicated by the Immutable NDL Schedule in the NDL Schedule Counter Proposal may not be overlapped with those indicated by the Immutable NDL Schedule in the NDL Schedule Initial Proposal.

Table 17. Key components in NAN Schedule Initial and Counter Proposals

NAN Schedule Initial Proposal in Data Path Request				**NAN Schedule Counter Proposal in Data Path Response (NDL status = Continued)**			
A. Conditional or Committed FAWs indicated by NAN Availability attributes	**B. Immutable NDL CRBs indicated by Immutable schedules in NDL attribute**	**C. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**Q. QoS Requirements indicated by NDL QoS attribute**	**D. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**E. Immutable NDL CRBs indicated by Immutable schedules (optional) in NDL attribute**	**S. QoS Requirements indicated by NDL QoS attribute**	**F. Conditional or Committed FAWs indicated by NAN Availability attributes**
Yes	No	No	No	Any selection	Any selection	Any selection	Superset of D, E, and S (if included)
Yes	Yes (subset of A)	No	No	Any selection	Any selection	Any selection	Superset of B, D, E, and S (if included)
Yes	No	Yes (subset of A)	No	Any selection	Any selection	Any selection	Superset of D, E, and S (if included)
Yes	Yes (subset of A)	Yes (subset of A)	No	Any selection	Any selection	Any selection	Superset of B, D, E, and S (if included)
Yes	No	No	Yes	Any selection	Any selection	Any selection	Superset of Q, D, E, and S (if included)
Yes	Yes (subset of A)	No	Yes	Any selection	Any selection	Any selection	Superset of B, Q, D, E, and S (if included)
Yes	No	Yes (subset of A)	Yes	Any selection	Any selection	Any selection	Superset of Q, D, E, and S (if included)
Yes	Yes (subset of A)	Yes (subset of A)	Yes	Any selection	Any selection	Any selection	Superset of B, Q, D, E, and S (if included)

When the NDP/NDL Initiator receives the Data Path Response NAF with the “Response” NDL attribute,

- If the Status subfield in the NDL attribute is set to “Accepted”, the NDP/NDL Initiator completes the NDL Schedule Setup. The established NDL is enrolled into the agreed NDC in the NDL Schedule Compliant Proposal. The NDP/NDL Initiator shall be present during its Committed FAWs, indicated by the NDL Schedule Initial Proposal. If the NDP/NDL Initiator indicates the Conditional FAWs in the NDL Schedule Initial Proposal, and if there are any overlapped portions between its Conditional FAWs and the NDP/NDL Responder’s Committed FAWs, those overlapped portions become its Committed FAWs
- If the Status subfield in the NDL attribute is set to “Rejected”, the NDP/NDL Initiator terminates both the NDP Setup and the NDL Schedule Setup. If the NDP/NDL Initiator indicates the Conditional FAWs in the NDL Schedule Initial Proposal, it may not be present during those FAWs. The NDP/NDL Initiator may retry the NDL Schedule setup based on the NDL Schedule Suggested Proposal, if any
- If the Status subfield in the NDL attribute is set to “Continued”, the NDP/NDL Initiator shall return a Data Path Confirm NAF to the NDP/NDL Responder

When the NDP/NDL Initiator transmits a Data Path Confirm NAF to the NDP/NDL Responder, it shall include a NDL attribute with the Type subfield set to “Confirm” and with the Status subfield set to either “Accepted” or “Rejected”.

If the Status subfield of the NDL attribute is set to “Accepted”, the Data Path Confirm NAF shall include a NDL Schedule Confirm Proposal (refer to Table 18).

- The NDL Schedule Confirm Proposal shall include one or more NAN Availability attributes with one or more Committed Availability entries, which shall indicate Committed FAWs that contain:
  - The NDC CRBs indicated by the proposed NDC in the NDL Schedule Counter Proposal
  - The NDL CRBs indicated by the Immutable NDL Schedule, if included in the NDL Schedule Counter Proposal
  - Sufficient NDL CRBs that fulfill the QoS requirements indicated by the NDL QoS attribute, if included in the NDL Schedule Counter Proposal
- The NDL Schedule Confirm Proposal shall also include the same NDC attribute as the proposed NDC attribute in the NDL Schedule Counter Proposal, with the Selected NDC flag set to one (1)

The Data Path Confirm NAF with a NDL Schedule Confirm Proposal may also include one or more S3 attributes.

If the NDP/NDL initiator accepts the proposed immutable NDL Schedule in the NDL Schedule Counter Proposal, then the preferred primary channel of the NDP/NDL initiator for the time slots in the accepted immutable NDL schedule shall be the same as the indicated preferred primary channel of the peer device for the proposed immutable NDL Schedule.

If the NDP/NDL initiator accepts the proposed NDC in the NDL Schedule Counter Proposal, then the preferred primary channel of the NDP/NDL initiator for the time slots in the accepted NDC shall be the same as the indicated preferred primary channel of the peer device for the proposed NDC.

Table 18. Key components in NAN Schedule Counter and Confirm Proposals

NAN Schedule Counter Proposal in Data Path Response				NAN Schedule Confirm Proposal in Data Path Confirm (NDL status = Accepted)	
A. Conditional or Committed FAWs indicated by NAN Availability attributes	**B. Immutable NDL CRBs indicated by Immutable schedules in NDL attribute**	**C. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**Q. QoS Requirements indicated by NDL QoS attribute**	**D. NDC CRBs indicated by NDC attribute with the Selected NDC flag set**	**E. Committed FAWs indicated by NAN Availability attributes**
Yes	No	Yes	No	Same as C	Superset of D
Yes	Yes (subset of A)	Yes (subset of A)	No	Same as C	Superset of B and D
Yes	No	Yes	Yes	Same as C	Superset of D and Q
Yes	Yes (subset of A)	Yes (subset of A)	Yes	Same as C	Superset of B, D, and Q

After the NDP/NDL Initiator transmits the Data Path Confirm NAF with the "Confirm” NDL attribute and the NDL Schedule Confirm Proposal, it completes its NDL Schedule setup and shall be present during its Committed FAWs, indicated by the NDL Schedule Confirm Proposal.

If the NDP/NDL Initiator transmits the “Confirm” NDL attribute with the Status subfield set to “Rejected” in the Data Path Confirm NAF, it terminates its NDP setup and the NDL Schedule setup. The NDP/NDL Initiator may not include any NAN Availability attributes in the NAF.

When the NDP/NDL Responder receives the Data Path Confirm NAF with the “Confirm” NDL attribute,

- If the Status subfield in the NDL attribute is set to “Accepted”, the NDP/NDL Responder completes the NDL Schedule Setup. The established NDL is enrolled into the proposed NDC in the NDL Schedule Confirm Proposal. The NDP/NDL Responder shall be present during its Committed FAWs, indicated by the NDL Schedule Counter Proposal. If the NDP/NDL Responder indicates the Conditional FAWs in the NDL Schedule Counter Proposal, and if there are any overlapped portions between its Conditional FAWs and the NDP/NDL Initiator’s Committed FAWs, those overlapped portions become its Committed FAWs
- If the Status subfield in the NDL attribute is set to “Rejected”, the NDP/NDL Responder terminates both the NDP Setup and the NDL Schedule Setup. If the NDP/NDL Responder indicates the Conditional FAWs in the NDL Schedule Counter Proposal, it may not be present during those FAWs

The NDP/NDL Initiator and the NDP/NDL Responder generate the DataConfirm event with the status set to “Accepted” when both the NDP setup and the NDL Schedule setup are completed successfully; otherwise, the DataConfirm event is generated with the status set to “Rejected” and with a Reason Code.

Figure 33 and Figure 34 illustrate the sequence of steps to carry out the NDP and NDL Schedule setup without the ND-TKSA.

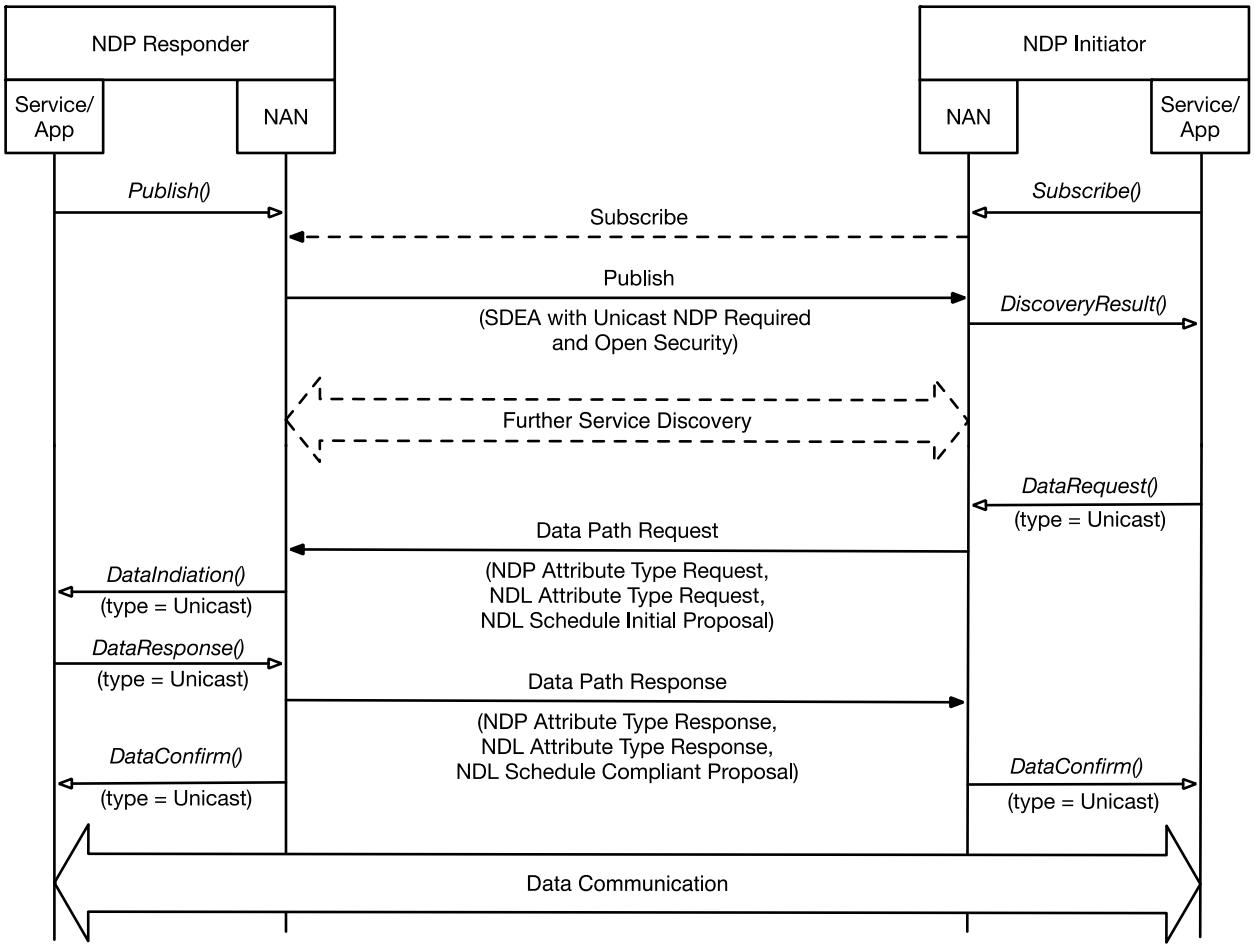


Figure 33. NDP and NDL Schedule setup without NDL Schedule Counter Proposal

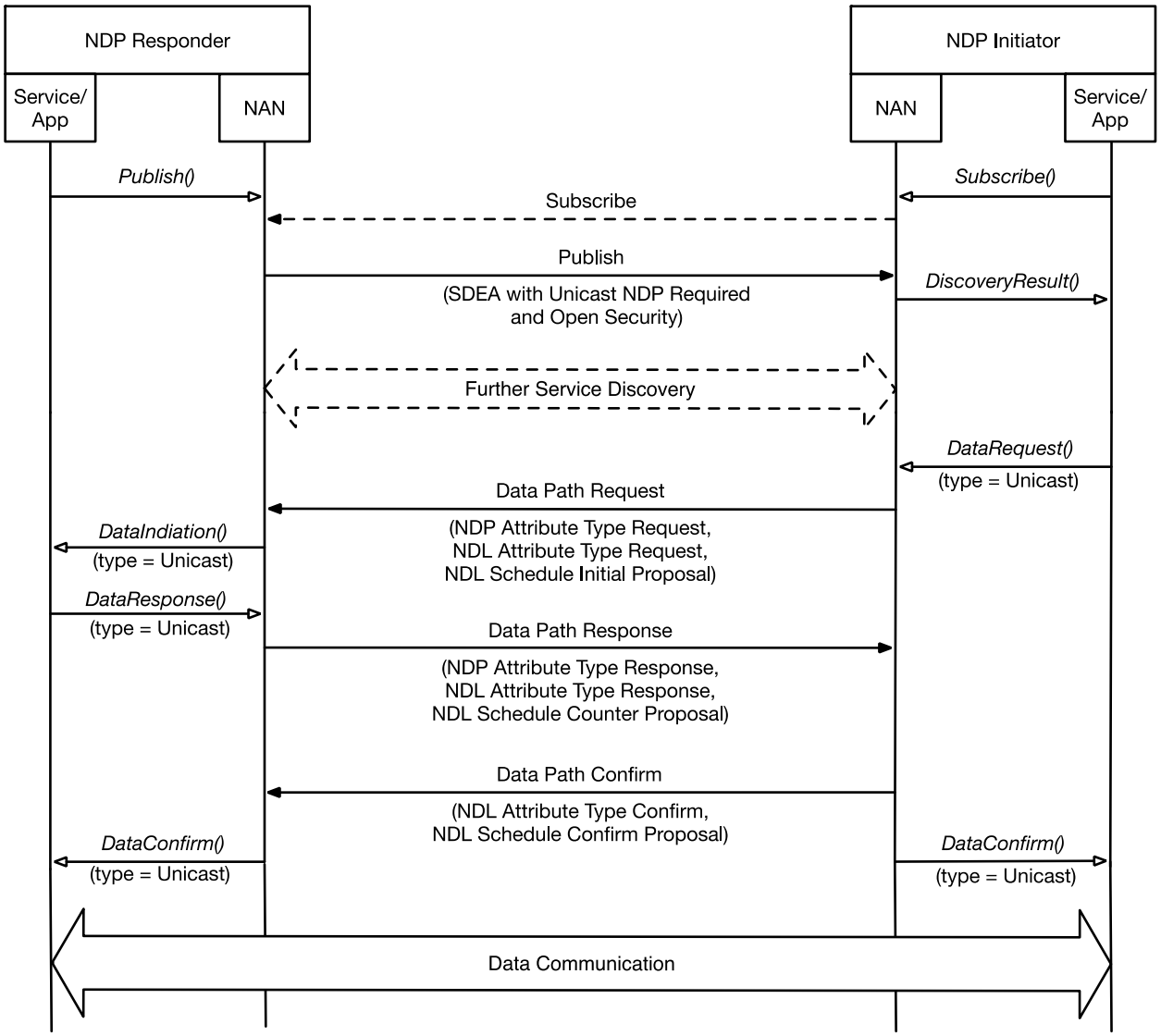


Figure 34. NDP and NDL Schedule setup with NDL Schedule Counter Proposal

Figure 35 illustrates an example of NDL Schedule Initial Proposal and NDL Schedule Compliant Proposal.

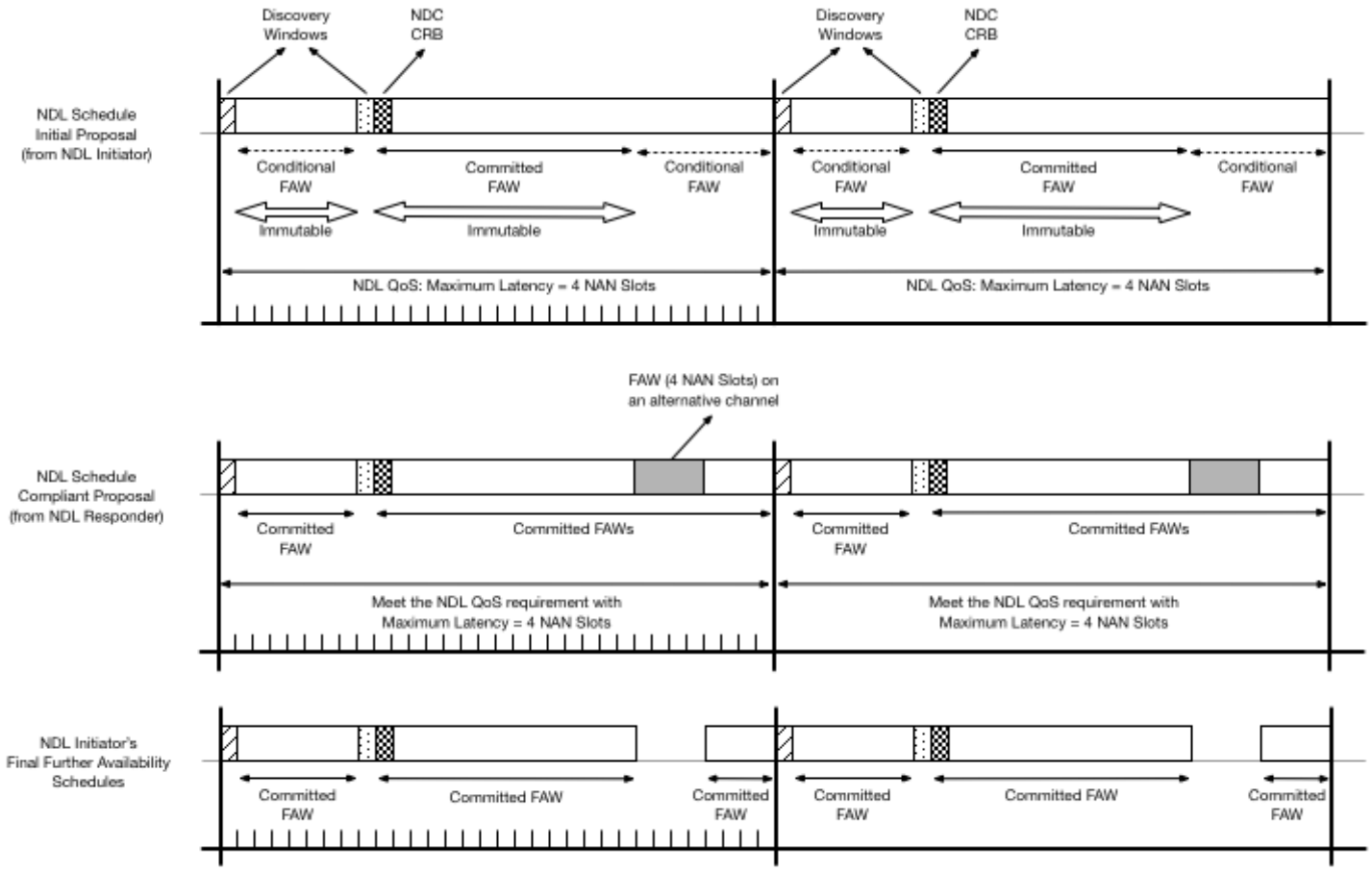


Figure 35. NDL Schedule Initial Proposal and Compliant Proposal

Figure 36 illustrates an example of NDL Schedule Initial Proposal, Counter Proposal, and Confirm Proposal.

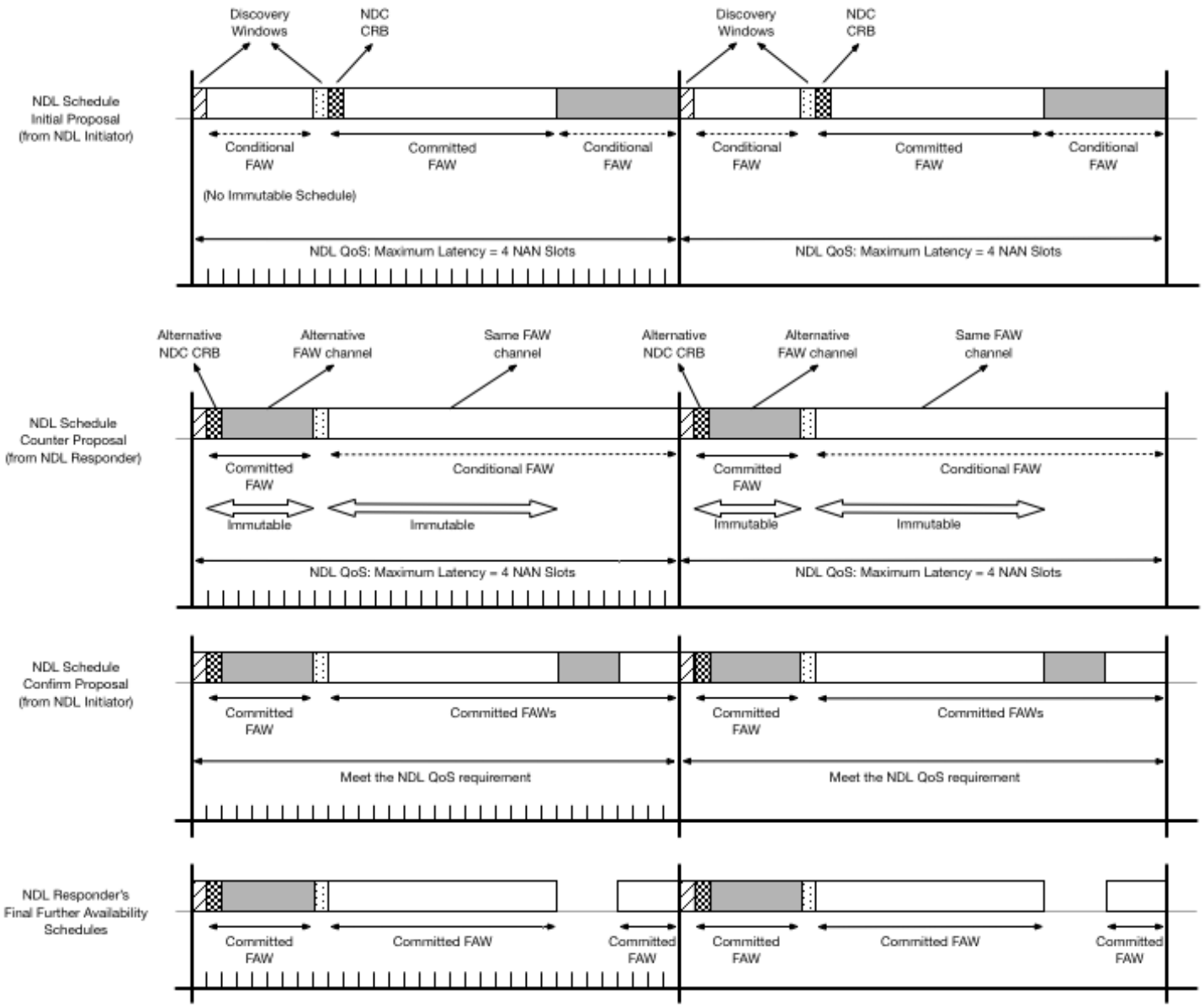


Figure 36. NDL Schedule Initial Proposal, Counter Proposal, and Confirm Proposal

NDP and NDL Schedule Setup with NDP Confirm Required

If the NDP/NDL Initiator sets the “Confirm Required” flag in the “Request” NDP/NDPE attribute in the Data Path Request NAF, and the NDP/NDL Responder accepts the NDP setup request and either accepts or counters the NDL setup request, the NDP/NDL Responder shall

- Set the Status subfield to “Continued” in the “Response” NDP/NDPE attribute in the Data Path Response NAF; and
- Wait for the “Confirm” NDP/NDPE attribute from the NDP/NDL Initiator before transmitting any data frames to the NDP/NDL Initiator

Table 19 summaries the relationship between the Status values in the NDP/NDPE attribute and the NDL attribute included in the Data Path Response NAF.

Table 19. Relationship between NDP Status and NDL Status in Data Path Response NAF with NDP Confirm Required

NDP Status	NDL Status		
	Accepted	**Continued**	**Rejected**
Continued	Allowed	Allowed	Not Allowed
Rejected	Not Allowed	Not Allowed	Allowed

In response to a received “Response” NDP/NDPE attribute with the Status subfield set to “Continued” in the Data Path Response NAF, the NDP/NDL Initiator shall return a Data Path Confirm NAF that includes the “Confirm” NDP/NDPE attribute.

- If the Data Path Response NAF includes the NDL attribute with the Status subfield set to “Accepted”, the NDP/NDL Initiator does not need to include the NDL attribute in the Data Path Confirm NAF
- If the Data Path Response NAF includes the NDL attribute with the Status subfield set to “Continued”, the NDP/NDL Initiator needs to include the “Confirm” NDL attribute in the Data Path Confirm NAF
- If the NDP/NDL Initiator needs to include both the “Confirm” NDL attribute and the “Confirm” NDP/NDPE attribute in the Data Path Confirm NAF, then the relationship between the Status values in the NDP/NDPE attribute and the NDL attribute included in the Data Path Confirm NAF are as given in Table 20

Table 20. Relationship between NDP Status and NDL Status in Data Path Confirm NAF with NDP Confirm Required

NDP Status	NDL Status	
	Accepted	**Rejected**
Accepted	Allowed	Not Allowed
Rejected	Not Allowed	Allowed

If the NDP/NDL Initiator transmits the Data Path Confirm NAF with the “Confirm” NDP/NDPE attribute, and the Status subfield of the NDP/NDPE attribute is set to “Accepted”, it completes its NDP setup and NDL Schedule setup; otherwise, both the NDP setup and the NDL Schedule setup are terminated.

When the NDP/NDL Responder receives the Data Path Confirm NAF with the “Confirm” NDP/NDPE attribute, and the Status subfield of the NDP/NDPE attribute is set to “Accepted”, it completes its NDP setup and NDL Schedule setup; otherwise, both the NDP setup and the NDL Schedule setup are terminated.

Figure 37 illustrates the sequence of steps to carry out the NDP and NDL Schedule Setup with NDP Confirm Required.

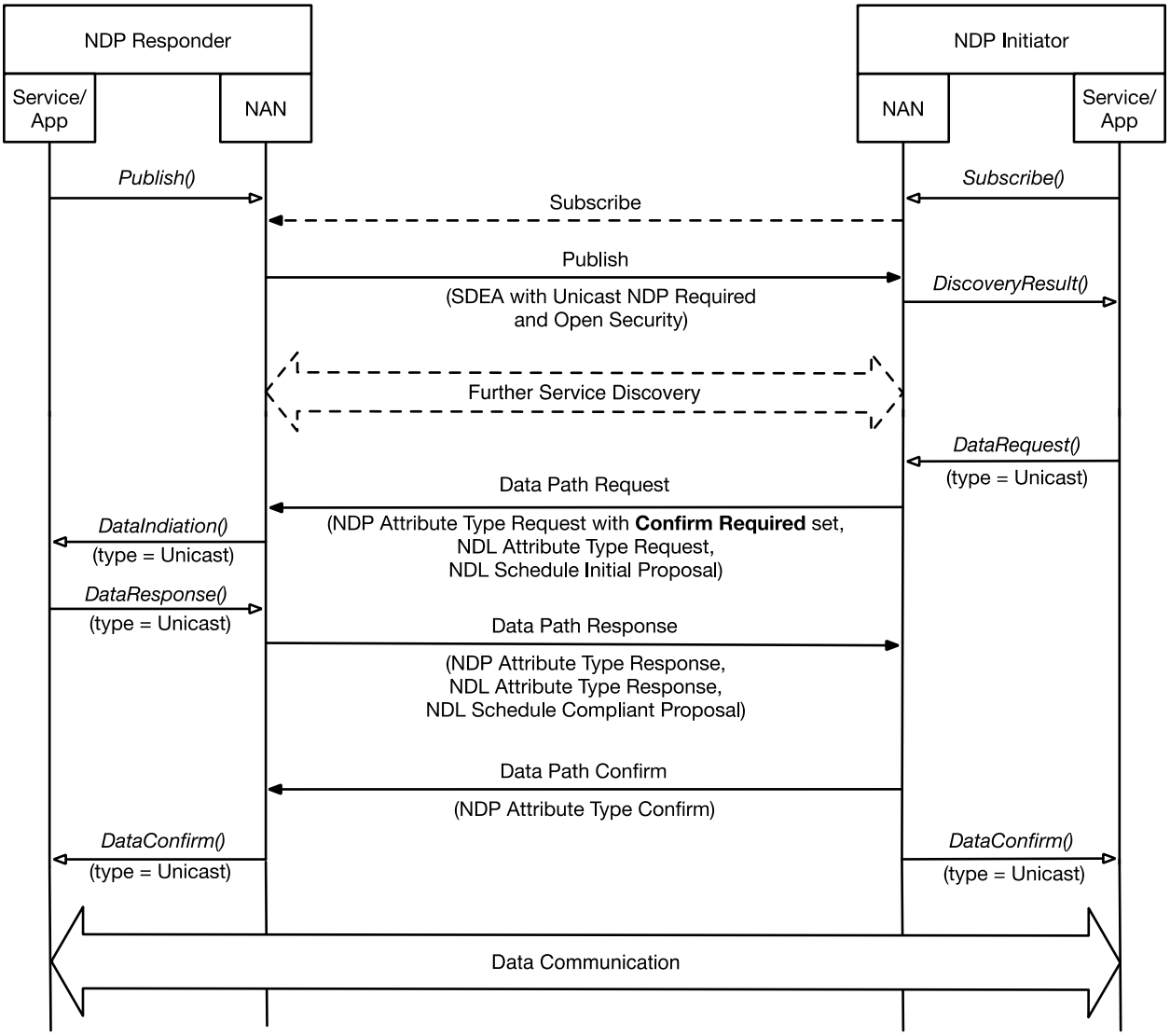


Figure 37. NDP and NDL Schedule Setup with NDP Confirm Required

NDP and NDL Schedule Setup with ND-TKSA

If a ND-TKSA is also started together with the NDP and NDL setup, the NDP/NDL Initiator and the NDP/NDL Responder shall also include the security attributes in the Data Path Setup NAFs, as specified in section 7.1.3.1.

The NDP/NDL Initiator and the NDP/NDL Responder generate the DataConfirm event with the status set to “Accepted” when the NDP setup, the NDL Schedule setup, and the ND-TKSA are successful and either NDL Schedule setup succeeded successfully or there is an existing NDL that was already setup; otherwise, the DataConfirm event is generated with the status set to “Rejected” and with a Reason Code.

Figure 38 illustrates the sequence of steps to carry out the NDP and NDL Schedule setup with the ND-TKSA.

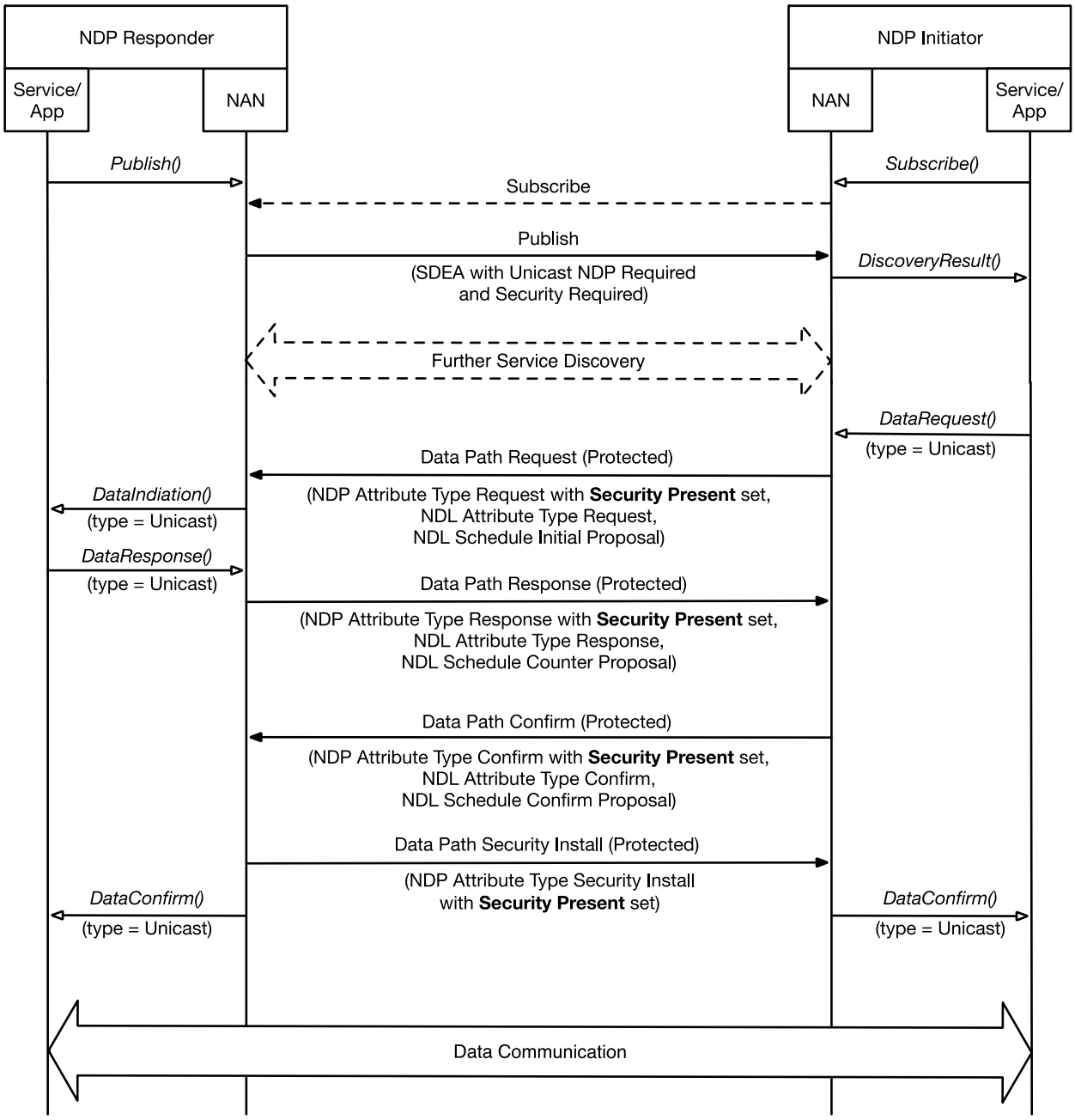


Figure 38. NDP and NDL Schedule Setup with ND-TKSA

For NCS-SK Cipher Suite, the Data Path Setup messages are protected using the MIC in the Security Key Descriptor attributes in the messages. In addition, if there is an existing ND-TKSA between the devices, these messages are encrypted using the corresponding encryption key. See section 7 for details on how the frames are protected.

6.2.3.4 NDL Schedule Update

Once a NAN Device establishes a NDL with a peer NAN Device, either NAN Device may initiate the NDL Schedule update at any time.

A NAN Device may use the NAN Beacon, Schedule Update Notification NAF, or any other unicast or broadcast NAN management frame to convey its updated availability schedules to one or more peer NAN Devices, as specified in section 5. The NDL Schedules between the NAN Device and its peer NAN Devices may be changed accordingly based on the NAN Device's new availability schedules and the peers' existing availability schedules. The NAN Device shall ensure the

new NDL schedules contain sufficient NDL CRBs to meet the requirements of the existing NDLs, except for the ones it will terminate or renegotiate NDL schedules by using NDL Schedule Setup Handshake.

A NAN Device may transmit a NDL QoS attribute to a peer NAN Device by using the Schedule Update Notification NAF or other unicast NAN management frame, which indicates the updated QoS requirements for the NDL Schedule between the two NAN Devices.

A NAN Device may transmit one or more S3 attributes to a peer NAN Device by using the Schedule Update Notification NAF.

A NAN Device may also use the NDL Schedule Setup Handshake to update the NDL Schedule with a peer NAN Device. The NAN Device that initiates the NDL Schedule Setup becomes the NDL Initiator, and the peer NAN Device becomes the NDL Responder. The two NAN Devices use Schedule NAFs to exchange NDL attributes and NDL Schedule Proposals, as specified in section 6.2.3.3.

The Schedule NAFs with NDL Schedule Proposals may include one or more S3 attributes.

The NDL Schedule Setup Handshake with NDL Schedule Counter Proposal is illustrated in Figure 39.

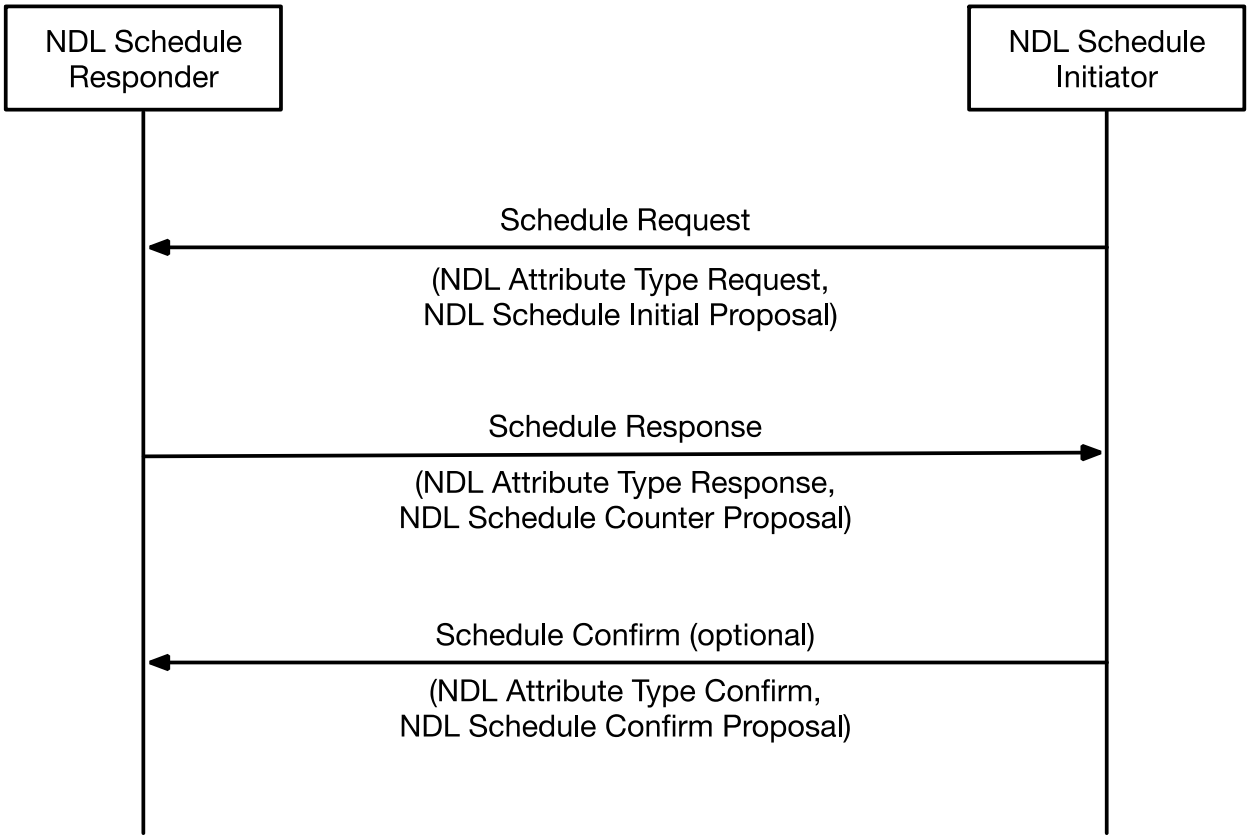


Figure 39. NDL Schedule Setup Handshake with NDL Schedule Counter Proposal

6.2.4 NDP and NDL setup failure and termination

Once a NAN Device pair establishes a NDP for a service instance, either device may terminate the NDP by transmitting a Data Path Termination NAF to the peer device. The Data Path Termination NAF shall include the NDP attribute with the Type subfield set to “Terminate”. The NAF may also include one or more NAN Availability attributes to indicate the NAF transmitter’s updated availability schedules.

A NAN Device may include the Max Idle Period field in the NDL attribute to indicate the time period during which a peer NAN Device refrains from transmitting over the NDL without being terminated.

If a NAN Device includes the Max Idle Period field in the NDL attribute, the NAN Device may terminate all the NDPs over the NDL established with the peer NAN Device if the NAN Device has not received any frame from the peer NAN Device for a time period greater than or equal to the time specified by the Max Idle Period field.

An S3 agreed with a peer terminates and becomes inapplicable when the corresponding NDL terminates or when a new NDL is negotiated.

A NAN Device should send a frame (ex. QoS Null frame) that requires a response to check the NDL connection established with the peer NAN Device before the NAN Device terminates the NDPs associated with the NDL due to not receiving any frame from the peer NAN Device.

For a device pair (A, B) with one or more NDPs established, device A shall update the availability of device B according to the latest availability in any NAN Action frame or Service Discovery frame received from device B, including any frames received as part of a failed NDP and/or NDL set up. The NDP Termination procedure is illustrated in Figure 40 and Figure 41.

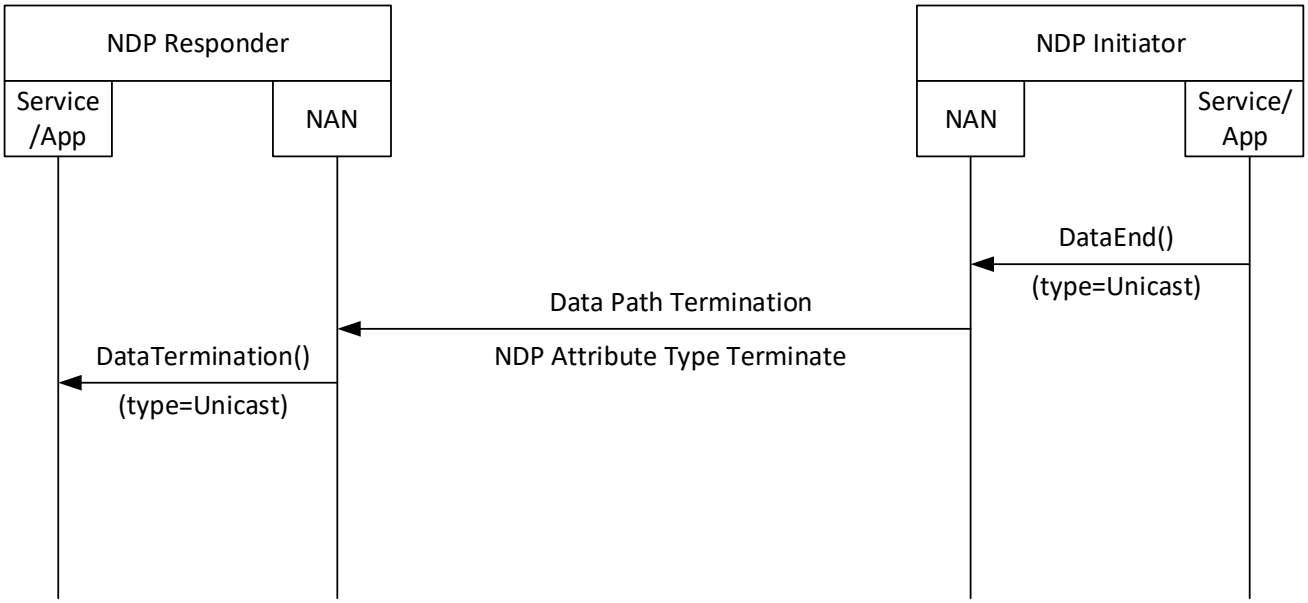


Figure 40. NDP Termination initiated by NDP Initiator

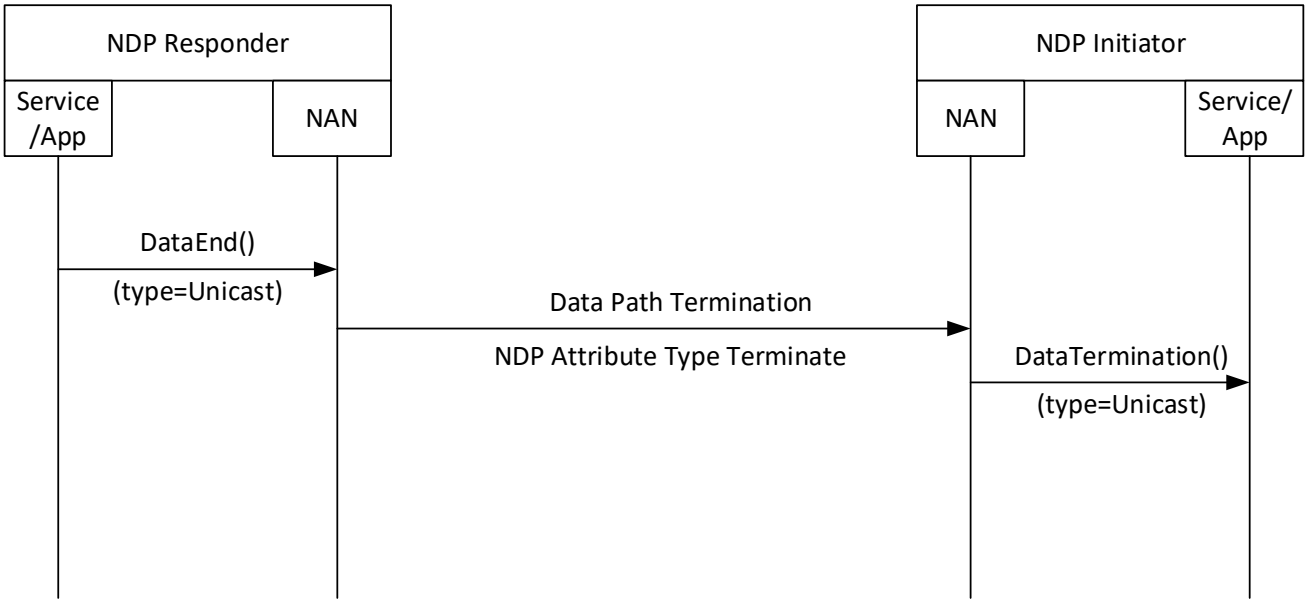


Figure 41. NDP Termination initiated by NDP Responder

6.2.5 NDP data frame filtering

When NAN Devices establish an NDP, corresponding NDIs are assigned to the NDP.

Upon NDP termination, the NDI assignment to the NDP is removed.

A NAN Device shall not transmit to the peer NAN Device any unicast NAN data frames other than those with A1 address and A2 address assigned to the NDP.

If a NAN Device receives a unicast NAN Data frame destined for it, but with A1 address and A2 address that are not assigned to the NDP, it shall discard the frame, and should send a Data Path Termination NAF to the frame transmitter.

6.2.6 NDL operations

There is one NAN Device Link (NDL) type: Synchronized NDL (S-NDL), which is defined in section 6.2.6.1.

6.2.6.1 S-NDL

A NAN Device that establishes a S-NDL with a peer NAN Device may transmit data frames to the peer from the beginning of each S-NDL CRB. If the NDL includes an S3, the NAN Device shall transmit data frames to the peer only during the available Sub Slots indicated by the S3.

All NAN Devices that support NDL operations shall support S-NDL.

6.2.6.2 NDL with unaligned schedule

If an agreed time block between two NAN devices overlaps with the unavailable duration indicated by the Unaligned Schedule attribute sent by either one of the two devices, then,

- Each duration contiguous in the time domain that is a portion of the original agreed time block and does not overlap with the unavailable duration is treated as a time block between the two devices
- The time block inherits the properties of the original time block. For example, if the original time block is S-NDL, then the time block is also S-NDL

If an announced time block from a NAN device overlaps with the unavailable duration indicated by the Unaligned Schedule attribute sent by the NAN device, then

- Each duration contiguous in the time domain that is a portion of the announced time block and does not overlap with the unavailable duration, is treated as a time block; and
- The time block inherits the properties of the original time block. For example, if the original time block is for further availability, then the time block is also for further availability

In the example in Figure 42 illustrating the operation of unaligned schedule indication, assume that two NAN Devices agree on time blocks 1, 2, and 3 on channel 1 and channel 2 as their NDL schedule. Assume that one of the two NAN Devices sends an Unaligned Schedule attribute.

NOTE: In Figure 42, the time duration indicated by Unaligned Schedule attribute may not align with the 16TU boundary defined by NAN for allocating time blocks. We illustrate three possible cases. In case 1, the Unaligned Schedule attribute does not include channel information. In case 2, the Unaligned Schedule attribute includes channel information on channel 2, and the Channel Availability field is set to one. In case 3, the Unaligned Schedule attribute includes channel information on channel 2, and the Channel Availability field is set to zero. The agreed time blocks under unaligned schedule indication are shown for three cases correspondingly in Figure 42.

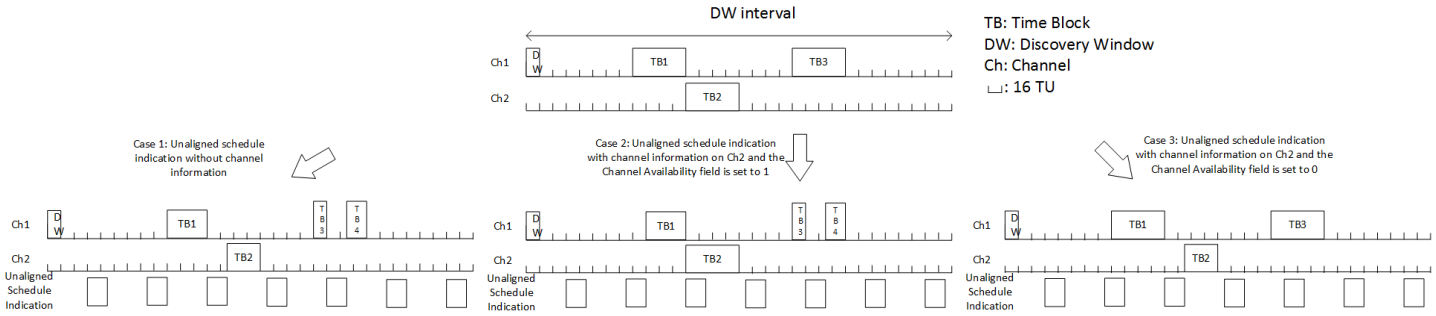


Figure 42. NDL with Unaligned Schedule example

6.2.7 TCP/IP bring-up using the NDPE attribute

A NAN Device indicates its support for the NDPE attribute by setting the NDPE attribute support subfield to 1 in the Capabilities field of the Device Capability attribute.

If a NDP Responder indicates its support for the NDPE attribute, for example, by including the Device Capability attribute with the NDPE attribute support subfield set to 1 in a Publish message, a NDP Initiator that also supports the NDPE attribute shall:

- Include a Device Capability attribute in the Data Path Request NAF with the NDPE attribute support subfield set to 1; and
- Include a NDPE attribute in the Data Path Request NAF

If the NDP Initiator includes the IPv6 Link Local TLV in the NDPE attribute,

- The NDP Initiator shall enable the corresponding IPv6 Link Local address for IP communication from the NDP Responder
- If the NDP Responder communicates with the NDP Initiator over IP, it shall use the corresponding IPv6 Link Local address provided by the NDP Initiator

If the NDP Initiator does not include the IPv6 Link Local TLV in the NDPE attribute,

- The NDP Initiator shall enable the IPv6 Link Local address derived from the Initiator NDI, as specified in Appendix J, for IP communication from the NDP Responder
- If the NDP Responder communicates with the NDP Initiator over IP, it shall use the IPv6 Link Local address derived from the Initiator NDI as specified in Appendix J

If a NDP Initiator indicates its support for the NDPE attribute and includes a NDPE attribute in a Data Path Request NAF transmitted to a NDP Responder, the NDP Responder that also supports the NDPE attribute shall include a NDPE attribute in the Data Path Response NAF.

If the NDP Responder includes the IPv6 Link Local TLV in the NDPE attribute,

- The NDP Responder shall enable the corresponding IPv6 Link Local address for IP communication from the NDP Initiator
- If the NDP Initiator communicates with the NDP Responder over IP, it shall use the corresponding IPv6 Link Local address provided by the NDP Responder

If the NDP Responder does not include the IPv6 Link Local TLV in the NDPE attribute,

- The NDP Responder shall enable the IPv6 Link Local address derived from the Responder NDI, as specified in Appendix J, for IP communication from the NDP Initiator
- If the NDP Initiator communicates with the NDP Responder over IP, it shall use the IPv6 Link Local address derived from the Responder NDI, as specified in Appendix J

A NDP Initiator may include both a NDP attribute and a NDPE attribute in a Data Path Request NAF transmitted to a NDP Responder. If the NDP Responder supports the NDPE attribute, it may ignore the NDP attribute included in the Data Path Request NAF.

A NDP Responder shall not include both a NDP attribute and a NDPE attribute in a Data Path Response NAF.

The NDP Responder may also transmit the transport protocol and port number to the NDP Initiator by:

- Including a Service Info TLV in the NDPE attribute of the Data Path Response NAF, and
- Setting the OUI field of the Service Info TLV to 0x50-6F-9A (Wi-Fi Alliance specific OUI), and
- Setting the Service Protocol Types field of the Service Info TLV to 2 (Generic), and
- Including a Transport Port sub-attribute in the Service Specific Info field of the Service Info TLV, and
- If needed, including a Transport Protocol sub-attribute in the Service Specific Info field of the Service Info TLV

Once the NDP Initiator obtains both the IP address and TCP/UDP port information from the Data Path Response NAF, it may initiate TCP/IP connection with the NDP Responder.

Figure 43 shows the TCP/IP bring up protocol by using the NDPE attribute.

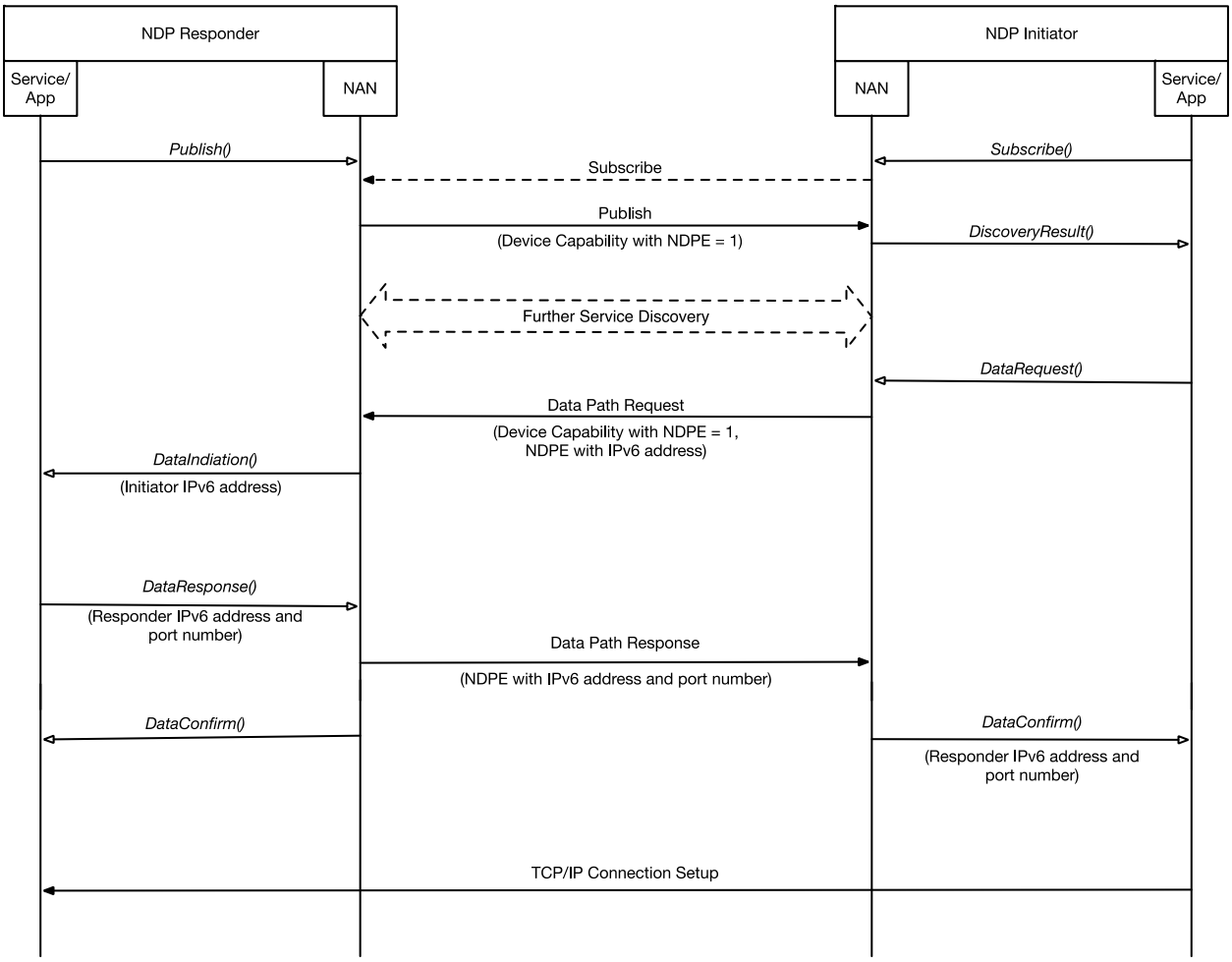


Figure 43. TCP/IP bring up using the NDPE attribute

6.2.8 NDP operations in 6 GHz

A NAN operation (e.g. NAN Data Path or NAN Ranging) in 6GHz may be realized through Very Low Power (VLP), Low Power Indoor (LPI) Client-to-Client (C2C), LPI or Standard Power (SP) communication. For example;

- In the case of VLP, NAN Devices can operate indoor and outdoor with a maximum Tx power of 14 dBm (CEPT)
- In the case of C2C, a given NAN Device can operate in this mode if it can hear and decode an enabling signal from an LPI AP. In this case, it can operate with higher maximum Tx power level of 24 dBm (CEPT). The additional 10 dB power level can greatly contribute to coverage or throughput
- In the case of LPI mode, NAN operation can be realized if one of the NAN Devices operates as a LPI AP. In this case, devices may operate at a higher power level of up to 24 dBm (CEPT) or 30dBm (US) for AP device, and 24 dBm (CEPT & US) for non-AP device

In the case of Standard Power mode, NAN operation can be realized only if one of the NAN Devices operates under supervision of the AFC System and comply with Fixed AFC (device has to be fixed) or Mobile AFC (device can be Mobile/Portable) device regulatory requirements. In this case devices may operate at a higher power level of up to 30 dBm for non-AP device and 36dBm for the AP device (USA).

A NAN Device supporting Wi-Fi 6 shall include the HE Capability element [19] in the Element Container attribute and a NAN Device supporting Wi-Fi 6E shall additionally include a DCEA in the NAN SDF frame, NAN Data Path Request/Response frame and NAN Ranging Request/Response frame. A NAN Device may set b0 of the Regulatory Info in the DCEA to 1 and set b1-b3 of the Regulatory Info to indicate a NAN operation mode in 6GHz band, as permitted by regulatory requirements. A NAN Device may also set b0 of the Regulatory Info in the DCEA to 0 to indicate the 6GHz operation mode information is not available. A NAN Device supporting Wi-Fi 6E may also include a Country Code attribute in NAN Beacons and SDF frames.

If a NAN Device operates as SP and/or LPI AP, a TPEA shall be included in the NAN Data Path Request/Response frame and NAN Ranging Request/Response frame, and may be included in NAN beacons and SDF frames. If the SP or LPI AP’s Regulatory Info has changed during the NAN operation (e.g., if it receives updated power limits from AFC that have changed, or is no longer under control of an AFC), the NAN Device shall notify its peer by transmitting NAN Beacon frames with a DCEA and a TPEA included, containing the corresponding new values.

When a NAN frame includes a TPEA, it shall also include at least one NAN Availability attribute with at least one channel entry. Each schedule entry of the TPEA shall be associated to one or more channel entries of the corresponding NAN Availability attribute. A NAN frame shall not include more than one TPEA.

If a NAN Device's Regulatory Info has changed during the NAN operation (e.g., moving from indoor to outdoor), the NAN Device shall notify its peer by transmitting the Schedule Update Notification frame with a DCEA included, containing the corresponding new values.

7 NAN security and privacy protection

7.1 NAN data path security

Security may be supported by a NAN service to:

- Authenticate a NAN peer and support link layer encryption of NAN Data Path unicast and management frames
- Protect the disclosure of Publish or Subscribed services
- Support link layer encryption of NAN Data Path multicast data frames
- Support integrity protection of multicast management frames
- Limit MAC address tracking to increase mobile user privacy
- Protect the service specific information shared in requests, responses, and announcements

The following sections provide recommendations for using NAN primitives with additional security.

7.1.1 NDP security setup

The security setup for a NDP is part of the data path setup. The setup process establishes the cryptographic keys necessary to protect transmitted information that allows:

- 802.11 encrypted unicast and multicast Data frames
- 802.11 Protected Management frames (PMF)
- Creation of Secure Service Identifiers

NDP security may setup a new ND-TKSA if one does not exist. It may use an existing ND-TKSA established between the peers. Multiple NDPs may share the same ND-TKSA.

7.1.2 Cipher suites

The NDP security setup supports multiple techniques to authenticate peer devices and establish appropriate cryptographic keys. Multiple cryptographic methods are supported using cipher suites that describe the set of algorithms and processing. The cipher suites may be based on either symmetric (shared secret key) or asymmetric (public/private keys) cryptographic techniques. The cipher suites are identified by Cipher Suite Identifiers (CSIDs).

The following cipher suites are defined for NDP security setup:

- NCS-SK-128, a pairwise 128-bit key derivation based on ownership of a shared symmetric key. The symmetric key derivation is out of scope of this specification, as specified in section 7.1.3.5. This cipher suite uses:
  - CCMP-128 for frame encryption
  - SHA-256 for the hash function used in PRF
  - HMAC-SHA-256 for KDF
- NCS-SK-256, a pairwise 256-bit key derivation based on ownership of a shared symmetric key. The symmetric key derivation is out of scope of this specification, as specified in section 7.1.3.5. This cipher suite uses:
  - GCMP-256 for frame encryption
  - SHA-384 for the hash function used in PRF
  - HMAC-SHA-384 for KDF
- NCS-PK-2WDH-128, a pairwise 128-bit key derivation based on a symmetric key. The symmetric key derivation based on two-way authenticated Diffie–Hellman key exchange, as specified in section 7.1.3.6. This cipher suite uses:
  - CCMP-128 for frame encryption
  - SHA-256 for the hash function used in PRF
  - HMAC-SHA-256 for KDF
- NCS-PK-2WDH-256, a pairwise 256-bit key derivation based on a symmetric key. The symmetric key derivation based on two-way authenticated Diffie–Hellman key exchange, as specified in section 7.1.3.6. This cipher suite uses:

  - GCMP-256 for frame encryption
  - SHA-384 for the hash function used in PRF
  - HMAC-SHA-384 for KDF
- NCS-GTK-CCMP-128, a 128-bit symmetric group key distributed to protect multicast data frames:
  - CCMP-128 is used for frame encryption
  - The key is randomly generated and unique per NDI on the distributing device
- NCS-GTK-GCMP-256, a 256-bit symmetric group key distributed to protect multicast data frames:
  - GCMP-256 is used for frame encryption
  - The key is randomly generated and unique per NDI on the distributing device
- NCS-BIP-128, a 128-bit symmetric group key distributed to protect multicast management frames, including Beacon frames:
  - BIP-CMAC-128 is used for frame integrity protection (see section 12.5.4 of [1]). The algorithm protects integrity of frames using an 8-byte cryptographic MIC
  - The key is randomly generated and unique per NMI on the distributing device
- NCS-BIP-256, a 256-bit symmetric group key distributed to protect multicast management frames, including Beacon frames:
  - BIP-GMAC-256 is used for frame integrity protection (see section 12.5.4 of [1]). The algorithm protects integrity of frames using a 16-byte cryptographic MIC
  - The key is randomly generated and unique per NMI on the distributing device
- NCS-PK-PASN-128, a pairwise 128-bit key derivation based on a symmetric key. The symmetric key derivation is based on PASN, as specified in section 7.1.3.6. This cipher suite uses:
  - CCMP-128 for frame encryption
  - SHA-256 for the hash function used in PRF
  - HMAC-SHA-256 for KDF
- NCS-PK-PASN-256, a pairwise 256-bit key derivation based on a symmetric key. The symmetric key derivation is based on PASN, as specified in section 7.1.3.6. This cipher suite uses:
  - GCMP-256 for frame encryption
  - SHA-384 for the hash function used in PRF
  - HMAC-SHA-384 for KDF

The cipher, hash function and KDF used with NCS-SK suites are denoted NCS-SK-CIPHER, NCS-SK-HASH, NCS-SK-KDF respectively.

7.1.3 NAN Security Associations

A NAN Security Association is an abstraction representing a set of security related parameters and cryptographic keys used to protect communications to one or more peer devices. Every NAN Security Association is bound to a local MAC address and a remote MAC address. There are multiple NAN Security Associations:

- NAN ND-TKSA between a local NDI MAC address and a unicast remote NDI MAC address of the peer and is used to protect unicast data and management frames
- NAN Group Addressed Data SA for a local or remote NDI MAC address which is used to protect group addressed data frames
- NAN Group Integrity SA for a local or remote NMI MAC address which is used to protect group addressed management frames
- NAN Beacon Integrity SA for a local or remote NMI MAC address which is used to protect NAN Beacon frames

7.1.3.1 NAN Pairwise Security Associations

A NAN Data Pairwise Security Association (ND-TKSA) encompasses the security parameters and keys negotiated for protecting NAN data or management frames. It contains:

- The local NDI MAC address
- The peer NDI MAC address
- A cipher suite agreed upon for the security and identified by a CSID
- Cryptographic keys that shall include:
  - An IEEE 802.11 ND-TK used to encrypt Management or Data frames
  - The ND-KEK used to protect security setup
  - The ND-KCK used to provide an integrity check for the security setup
- A transmit key ID if the SA is for local NDI address

A Security Association for a symmetric cipher suite shall include:

- A shared symmetric key (ND-PMK)
- A list of NDPIDs associated with the security association
- The SCID used to identify the context of the security setup and identifies the long-term keys used to establish the Security Association
- Security Association lifetime
- Key Replay Counters for Data and Management SAs

A ND-TKSA is equivalent to the PTKSA defined in [1] section 12.6.1.1.6.

NAN supports multiple ND-TKSAs between a pair of NAN devices. A ND-TKSA is established between a pair of Data Interfaces addresses negotiated during NDP setup between Service Instance peers. In some cases, the Data Interface address may be set to the NMI address. There is at most one ND-TKSA between a pair of addresses.

A NAN ND-TKSA shall not use cipher suites BIP-CMAC-128 and BIP-GMAC-256.

7.1.3.2 NAN Group Addressed Data Security Associations

A NAN Group Addressed Data Security Association is equivalent to a GTKSA defined in section 12.6.1.1.8 of [1]. The GTKSA is used to protect group addressed data frames to one or more NAN peers. It contains:

- Cryptographic keys used to protect group addressed data frames. The keys are cryptographically random and generated by the device identified by the GTKSA
  - A key identifier (Key ID) is maintained with each key. It shall take the values 1 or 2
- A NAN Cipher Suite agreed upon and identified by a CSID
- A local or remote NDI MAC address. A GTKSA with the local MAC address is used for transmitting protected frames where as a GTKSA with a remote MAC address is used for receiving protected frames
- A transmit key ID if the SA is for local NDI address
- Key Replay counters for each key

If the device supports GTKSA and is required to enable GTK protection for one or multiple services, it shall create at least one GTKSA for transmit. There is exactly one GTKSA with a given NDI MAC address.

A Group Addressed Data SA shall not use cipher suites BIP-CMAC-128 and BIP-GMAC-256.

Note: Some service may request to use a private NDI (not shared with other services), in order to obtain exclusive protection.

Note: If the device needs to transmit unprotected group-addressed data frames, it shall use an NDI not associated with any GTKSA (for transmit).

When a device establishes an NAN Data Path with a peer, which also supports a GTKSA:

- If a device serves as an NDP Initiator, it shall include a GTK KDE in the NAN Shared Key Descriptor attribute of the Data Path Confirm message defined in section . Otherwise, it shall include the KDE in NAN Shared Key Descriptor attribute of the Data Path Security Install message defined in section 9.5.21.5
- After a device and the peer receive the GTK from each other, they shall create the respective GTKSA for receive

Once the NAN Data Path Setup is completed successfully, both the device and the peer are able to send and receive protected group addressed data frames from each other.

7.1.3.3 NAN Group Integrity Security Associations

A NAN Group Integrity Security Association is equivalent to a IGTKSA defined in [802.11-2020] § 12.6.1.1.9. The IGTKSA is used to protect group addressed management frames, other than Beacon frames. It contains:

- Cryptographic keys used to protect forementioned management frames. The keys are cryptographically random and generated by the device identified by the IGTKSA.
  - A key identifier (Key ID) is maintained with each key. It shall take the values 4 or 5
- A NAN Cipher Suite agreed upon and identified by a CSID
- A local or remote NMI MAC address. An IGTKSA with the local MAC address is used for transmitting protected frames where as an IGTKSA with a remote MAC address is used for receiving protected frames.
- A transmit key ID if the SA is for local NMI address
- A single replay counter for each key

There is exactly one IGTKSA with a given NMI MAC address.

A group integrity SA shall only use BIP-CMAC-128 or BIP-GMAC-256.

When a device establishes an NAN Data Path with a peer, which also supports a IGTKSA:

- If a device serves as an NDP Initiator, it shall include a IGTK KDE in the NAN Shared Key Descriptor attribute of the Data Path Confirm message defined in section 9.5.21.5. Otherwise, it shall include the KDE in NAN Shared Key Descriptor attribute of the Data Path Security Install message defined in section 9.5.21.5
- After a device and the peer receive the IGTK from each other, they shall create the respective IGTKSA for receive

Once the NAN Data Path Setup is completed successfully, both the device and the peer are able to send and receive protected group management frames from each other.

7.1.3.4 NAN Beacon Integrity Security Associations

A NAN Beacon Integrity Security association is equivalent to a BIGTKSA defined in section 12.6.1.1.11 of [1]. The BIGTKSA is used to protect Beacon frames. It contains:

- Cryptographic keys used to protect forementioned management frames. The keys are cryptographically random and generated by the device identified by the BIGTKSA
  - A key identifier (Key ID) is maintained with each key. It shall take the values 6 or 7
- A NAN Cipher Suite agreed upon and identified by a CSID
- A local or remote NMI MAC address. A BIGTKSA with the local MAC address is used for transmitting protected frames where as a GTKSA with a remote MAC address is used for receiving protected frames.
- A transmit key ID if the SA is for local NMI address
- A single replay counter for each key

There is exactly one BIGTKSA with a given NMI MAC address.

A Beacon integrity SA shall only use BIP-CMAC-128 or BIP-GMAC-256.

When a device establishes an NAN Data Path with a peer, which also supports a BIGTKSA:

- If a device serves as an NDP Initiator, it shall include a BIGTK KDE in the NAN Shared Key Descriptor attribute of the Data Path Confirm message defined in section 9.5.21.5. Otherwise, it shall include the KDE in NAN Shared Key Descriptor attribute of the Data Path Security Install message defined in section 9.5.21.5
- After a device and the peer receive the BIGTK from each other, they shall create the respective BIGTKSA for receive
- Once the NAN Data Path Setup is completed successfully, both the device and the peer are able to send and receive protected Beacon frames from each other.NAN security association setup

7.1.3.5 NAN Shared Key Cipher Suite

NAN Shared Key Cipher Suite (NCS-SK) is used to setup NAN security for protecting NAN frames when peers negotiating security have a shared key. When NCS-SK is selected for a ND-TKSA, the peers each know a shared key (ND-PMK) and their knowledge of the ND-PMK is confirmed by the NAN Data Path setup negotiations, similar to the 802.11 4-way handshake (refer to [1] section 12.7.6.4). Unlike the ND-PMK in the IEEE 802.11 standard, a NAN PMK, henceforth PMK, is bound to the Service Instance peers rather than MAC addresses used for exchanging NAN Management or Data frames.

NAN devices supporting security shall support NCS-SK-128.

Establishment of ND-PMK or derivation of ND-PMK from a passphrase is outside of the scope of the specification of NCS-SK. The ND-PMK may be established using another cipher suite that is able to derive a ND-PMK or installed by a network service.

When NCS-SK is used to set up NAN Security Association:

- ND-PMK used shall be of length 32 octets
- Protection of unicast Data frames, and unicast Management frames shall use NCS-SK-CIPHER keys. This is equivalent to the RSNA cipher suite selector 00-0F-AC-04 (CCMP-128) for 128 bit keys and 00-0F-AC-09 (GCMP-256) for 256 bit keys (refer to [1] Table 9-131)
- Protection of broadcast and multicast Management frames is not supported if the corresponding security associations (GTKSA, IGTKSA, BIGTKSA) are established as part of ND-TKSA setup or NAN pairing setup
- If group addressed data frame protection is required, one of the Cipher Suites for the GTKSA (NCS-GTK-*) shall be included in the Cipher Suite attribute field contained in the Cipher Suite Information attribute. Group addressed data frame protection is required if a device sets the ‘GTK Required’ subfield to 1 for the service (in SDEA control field) and the NDP (NDPE control field)
- To accommodate a peer NAN Device which does not support the NCS-GTK cipher suites, a NAN Device may either disable its GTKSA or support secured multicast (data) and non-secured multicast (data) on different NDIs
- Management frames, in particular those action frames specified as robust in (refer to [1], Table 9-47 Category Values) shall be protected
- Key derivation function (KDF) RSNA NCS-SK-KDF shall be used to derive key material of required length in bits (refer to [1] section 12.7.1.7.2) where PRF-<length> denotes NCS-SK-KDF-<length> in key derivation
- NAN Shared Key Descriptor attribute shall be included in the NDP setup messages for NAN ND-TKSA establishment
- SCIA containing ND-PMKID shall be included in NDP setup and response messages
- If encrypted data is carried in key descriptor elements in the NAN Shared Key descriptor, it shall use a ND-KEK of the same length as NCS-SK-CIPHER and the NIST AES Key Wrap algorithm [5]]. The encrypted data carries:
    - GTK KDE corresponding to the current GTK if and only if the device and the peer support GTKSA functionality. The KDE shall be included if ‘GTK Required’ in SDEA control for the service is set to 1
    - IGTK KDE corresponding to the current IGTK if the device and the peer support IGTKSA for their local NMI. The KDE shall be included if and only if both the devices advertise IGTKSA support in the Cipher Suite Information attribute
    - BIGTK KDE corresponding to the current BIGTK if the device and the peer support BIGTKSA for their local NMI. The KDE shall be included if and only if both the devices advertise BIGTKSA in the Cipher Suite Information attribute

  NOTE: The format of GTK KDE, IGTK KDE, and BIGTK KDE and the NAN Key Lifetime KDE are defined in section 9.5.21.5 (NAN Shared Key Descriptor – NAN KDE). KDEs shall be carried only in the encrypted data and never in the clear.

- Replay detection is provided for protected frames using the appropriate replay counter(s). The number of supported Replay Counters a ND-TKSA or a GTKSA supports are advertised in Cipher Suite Information attribute

To protect the integrity of NDP negotiation, the NAN Shared Key descriptor, the KCK, KEK, and MIC are as given in Table 21.

Table 21. NCS-SK Integrity Protection Parameters

Cipher suite	Integrity algorithm	ND-KCK_bits	Size of MIC	Key-wrap algorithm	ND-KEK_bits
NCS-SK-128	HMAC-SHA-256	128	16	NIST AES Key Wrap	128
NCS- SK-256	HMAC-SHA-384	192	24	NIST AES Key Wrap	256

NCS-SK Pairwise Key Derivation

The initiator of NDP setup shall take on the RSNA Authenticator role and the responder shall take the role of a RSNA Supplicant.

NAN Pairwise key derivation shall use the RSNA pairwise key hierarchy (refer to section 12.7.1.3 of [1]) using Nonce values obtained from NDP negotiation messages where the mapping from ND-PMK to ND-TK is accomplished using

PRF-Length (ND-PMK, “NAN Pairwise key expansion”, IAddr || Raddr || Inonce || Rnonce)

Where:

- IAddr and RAddr are NDP Initiator and NDP Responder MAC addresses respectively
- INonce and RNonce are Nonce values sent by the initiator and responder respectively

The ND-TK shall be derived from the ND-PMK using the above function, where its length is based on

- ND-KCK_bits + ND-KEK_bits + ND-TK_bits (refer to section 12.7.1.3 of [1])

The values of ND-KCK_bits and ND-KEK_bits are AKM suite dependent which is NIST AES Key Wrap, see Table 12-8 of [1]. The lengths of the ND-KCK and ND-KEK are given in Table 21.

ND-TK_bits is cipher-suite dependent (defined in Table 12-4 [1] Cipher suite key lengths) is 128-bits for NCS-SK-128 and 256 bits for NCS-SK-256.

With each negotiation, a ND-TK shall be derived with the negotiated Data Interface addresses. Data path setup and update negotiation NAFs are protected and validated using the ND-KCK and ND-KEK derived in the ND-PTK derivation process.

The Temporal Key (ND-TK) used for protection of NAN Action frames is described in section 7.3.2.

The ND-PMKID used in NAN Shared Key descriptor shall be derived using the following formula

ND-PMKID = L(HMAC-Hash (ND-PMK, “NAN PMK Name” || IAddr || RAddr || Service ID), 0, 128)

Where:

- IAddr and RAddr are the NDP Initiator and NDP Responder respectively. IAddr is set to ff:ff:ff:ff:ff:ff when ND-PMKID is included in publish messages
- Service ID is the Service ID of the service providing the ND-PMK
- HMAC-Hash is the hash function specific to the cipher suite as specified in section 7.1.2. For example, when the cipher suite used is NCS-SK-128, HMAC-Hash is HMAC-SHA-256

Management Interface and Data Interface addresses shall not change for the lifetime of an NDP.

NCS-SK security negotiation

When NCS-SK is used as the cipher suite for the security setup, Figure 44 illustrates the message flow using NAN Publish/Subscribe messages for advertising the supported cipher suites and available Security Context Identifiers to allow the inclusion of cipher suite proposals, supported Security Context Identifiers and their confirmation as part of NDP negotiation.

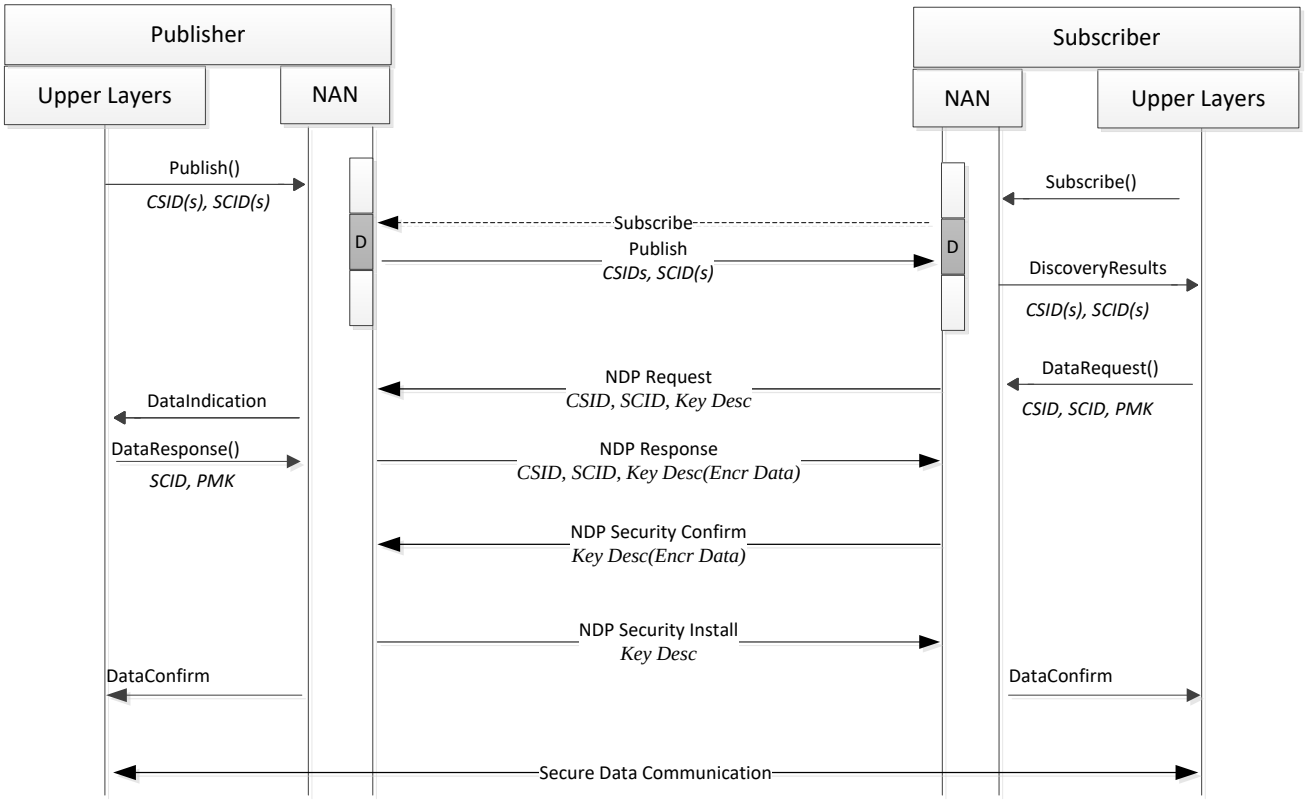


Figure 44. NAN Security Publish/Subscribe message flow

A NAN publisher shall advertise supported cipher suites and available SCIDsin NAN Publish messages. The initiating NAN Device, i.e., Subscriber, selects a suitable cipher suite and SCID for conducting the NDP negotiation and establishing the NAN ND-TKSA. If required, any GTKSA, IGTKSA and BIGTKSA shall have been established with the corresponding interface for the MAC address (NDI or NMI) is created. . The rest of this section details the security related aspects of the negotiation when NCS-SK Cipher Suite is selected.

The message flow used with NCS-SK to establish a NAN ND-TKSA follows closely the RSNA 4-way handshake as specified in section 12.7.6 of [1]. Unlike the RSNA 4-way handshake where the 802.11 key descriptor is carried in EAPOL frames, the 802.11 NCS-SK key descriptor is carried in the NAN Shared Key Descriptor attribute that shall be included in NDP negotiation messages. The contents of the key information field in the descriptor with NCS-SK have the same semantics as the 802.11 key descriptor.

- The version of 802.11 key descriptor shall be zero, indicating the use of AES CMAC and NIST AES Key Wrap
- Key type shall be set to Pairwise
- Install, Key ACK, Key MIC, Secure and Encrypted data bits have the same semantics as in RSNA
- All other bits are not used and set to zero
- GTK, IGTK and BIGTK, if required, are distributed using the corresponding KDEs. When keys are included in the Key Data field of the descriptor, Encrypted data bit shall be set and the Data field shall be encrypted

The four messages M1, M2, M3, and M4 in the RSNA 4-way handshake (refer to section 12.7.6.4 [1]) correspond in NAN to NDP request, NDP response, NDP Confirm and NDP Security Install messages. The key descriptor for NCS-SK shall be initialized as specified for the corresponding RSNA message with any NAN specific changes outlined in this section. The behavior of the Authenticator (Initiator) and the Supplicant (Responder) upon transmission or reception of these messages shall conform to RSNA description unless otherwise specified here.

The following fields in the key descriptor are not used, and set to zero on transmit and ignored on reception, when NCS-SK is used.

- Key length, because the length of various keys is already identified by the cipher suite
- EAPOL Key IV, because it is not needed with NIST AES Key Wrap (Default IV)
- Key RSC unless GTK is being distributed, in which case it shall contain the corresponding RSC for the key

NDP messages shall be checked for replays by the Supplicant using the Key Replay Counter in the descriptor and incremented by the Authenticator (NDP Initiator) before including in an NDP frame that carries the key descriptor. The replay counter is initialized to zero upon creation of the Management SA between the devices.

It is possible that multiple NAN shared key descriptors are part of a frame, each attempting a separate SA setup. In such a case, the MIC in each descriptor is constructed and updated over the entire frame in the order in which the descriptors appear in the frame.

M1 construction for NCS-SK

M1 shall contain the Cipher Suite attribute containing the NCS-SK, the SCIA containing the ND-PMKID, and the NAN Shared Key descriptor attribute along with other attributes needed in NDP establishment. The Cipher Suite attribute shall also contain the Cipher Suite ID for the GTKSA, if a GTKSA is required to protect group addressed data frames the device transmits. The key descriptor is initialized as specified for RSNA.

The fields in M1 following the Key Nonce may be omitted by the Initiator and ignored by the Responder.

M2 construction for NCS-SK

M2 shall contain the Cipher Suite attribute containing the NCS-SK, the SCIA containing the PMKID, and the NAN Shared Key descriptor attribute along with other attributes needed in NDP establishment. The Cipher Suite attribute shall also contain the Cipher Suite ID for the GTKSA, if a GTKSA is required to protect group addressed frames the device transmits. The key descriptor is initialized as specified for RSNA except,

- Key MIC is computed over the body of M2 (with Key MIC field initialized to zeros) that includes additional NAN attributes used for NDP setup
- Key Data Length will be zero for unicast M2
- A NAN Key Lifetime KDE specifying the lifetime of ND-TKSA may be included in the key data

M3 construction for NCS-SK

M3 shall contain the NAN Shared Key descriptor attribute along with other attributes needed in NDP establishment. The key descriptor is initialized as specified for RSNA except

- Key MIC is computed over the concatenation of an Authentication Token and the body of M3 that validates security and non-security attributes that are exchanged as part of NDP setup
- A NAN Key Lifetime KDE specifying the lifetime of ND-TKSA may be included in the key data
- Key RSC is set to 0 unless GTK KDE is included in the encrypted data of the descriptor

If any combination of GTKSA, IGTKSA, or BIGTKSA is required to protect group addressed data, multicast management frames the device transmits, the corresponding GTK, IGTK, and BIGTK KDEs are included in the encrypted data of the key descriptor. Key RSC is set to the RSC for the GTK when GTK KDE is included. The corresponding NAN Key Lifetime KDEs (see section 9.5.21.5 (NAN Shared Key Descriptor – NAN KDE)) may also be optionally included.

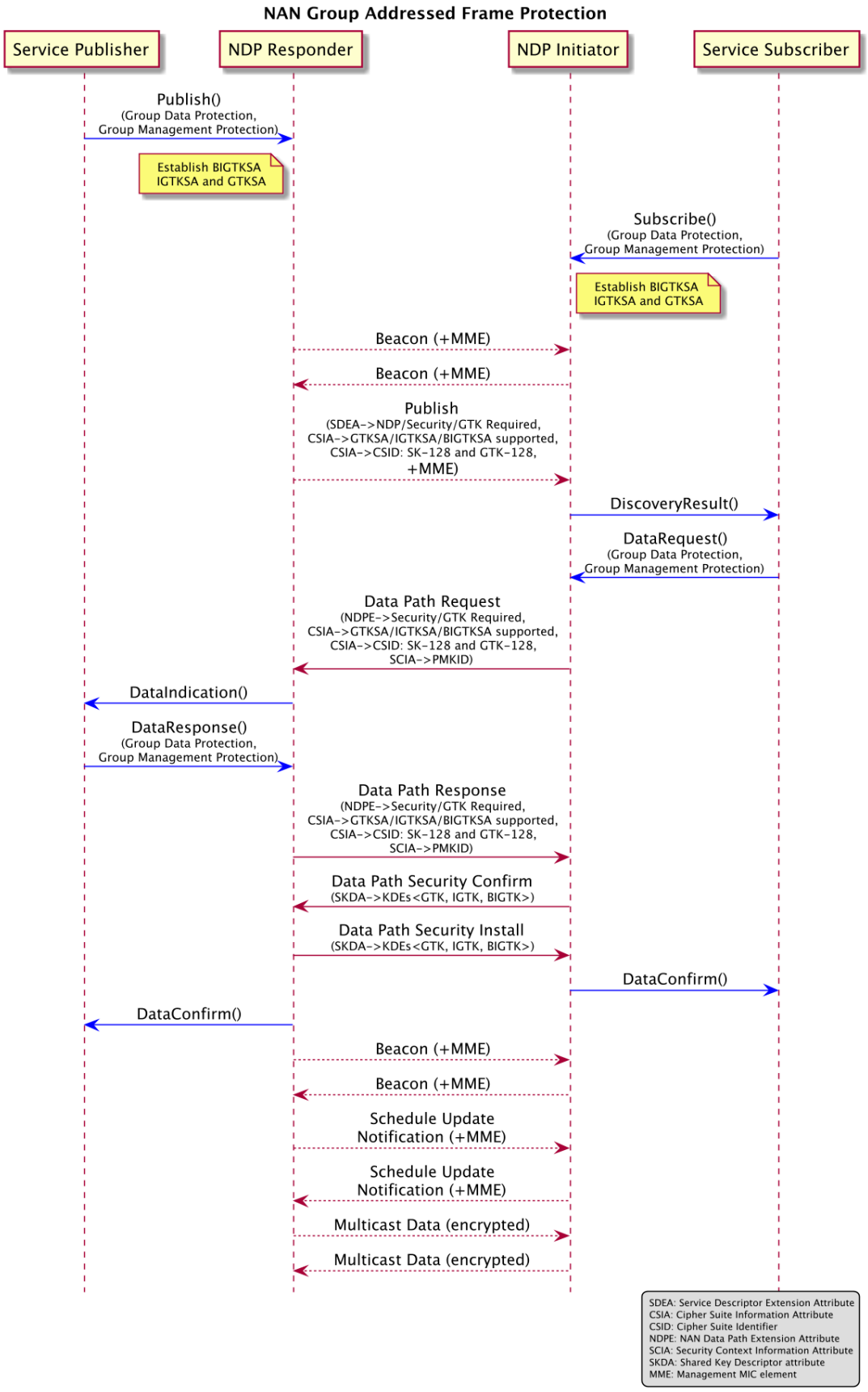


Figure 45. Example of group addressed frame protections

The Authentication Token included in the MIC, which provides for a secure confirmation of information sent by the Initiator, is computed as

L(NCS-SK-HASH(Authentication Token Data), 0, 128)

Where Authentication Token Data is the body of M1.

If the key lifetime value that is included in M3 is different from the value in M2, the minimum value from these values are used for key lifetime. If only one of M2 and M3 messages contains the NAN Key Lifetime KDE with the ND-TK's lifetime, the specified lifetime value is taken. If neither M2 nor M3 contains the NAN Key Lifetime KDE with the ND-TK's lifetime, the SA is deleted when all the NDPs using the SA are terminated.

M4 construction for NCS-SK

M4 shall contain the NAN Shared Key descriptor attribute with the install bit set, and the MIC is computed over the body of M4. The key descriptor is initialized as specified for RSNA except:

- If any combination of GTKSA, IGTKSA, or BIGTKSA is required to protect group addressed data, multicast management frames the device transmits, the corresponding GTK, IGTK, and BIGTK KDEs are included in the encrypted data of the key descriptor. The corresponding GTK, IGTK, and BIGTK Key Lifetime NAN KDEs (see § 9.5.21.5 (NAN Shared Key Descriptor – NAN KDE)) may also be optionally included
- Key RSC is set to the RSC for the GTK when GTK KDE is included

Figure 45 illustrates the message flows to enable group addressed frame protections.

NOTE: It is possible to setup a ND-TKSA, IGTKSA, and BIGTKSA when NAN pairing setup and/or verification is used without setting up NAN Data Path. Such SAs can be used to protect the discovery frames and possibly verify management frames received prior to the SA setup.

7.1.3.6 NAN Public Key Cipher Suite

When a NAN Public Key Cipher Suite (NCS-PK) is selected for a NAN ND-TKSA, the peers use an asymmetric (public/private keys) cryptographic technique to derive a symmetric key (ND-PMK) for a service instance and the ND-PMK is confirmed by the NAN Data Path setup negotiations, similar to the 802.11 4-way handshake (refer to [1], section 12.7.6.4).

When a NAN Public Key Two-Way Diffie–Hellman Cipher Suite (NCS-PK-2WDH) is selected, the peers use an OOB manner, such as the NFC Negotiated Connection Handover protocol (refer to section 12.1), to conduct two-way authenticated Diffie–Hellman key exchange. The shared secret established by the Diffie–Hellman key exchange is then used to derive ND-PMK and ND-PMKID, as specified in [18]. Once the ND-PMK is installed by the peers, the remaining security association protocol and algorithms are the same as those of the corresponding NCS-SK cipher suite, as specified in section 7.1.3.5.

NOTE: The ND-PMKID derivation method of NCS-PK-2WDH is different from that of NCS-SK.

7.1.4 Security groups

A group of devices can use the NAN Publish and Subscribe functions in a secure manner by providing each member of a NAN Security Group with a shared NAN Group Key. A device may be a member of multiple NAN Security Groups each with a different NAN Group Key. The creation and distribution of these keys to group members is outside the scope of this specification.

7.2 Privacy for NAN Service Identifiers

NAN devices that are members of a NAN Security Group create new a pseudo random Service ID for the discovery of their private services. For each NAN service supported within the NAN Security Group, the Service Name of each of the protected services within the group is transformed to a Secure Service ID using the NAN Group Key. Devices in the same group recognize the Secure Service ID and process it as the service represented by the originating Service Name. The untransformed Service ID formed from the Service Name may still be used to publish and subscribe the service to peers that are not part of the same NAN Security Group. Typically, this transitional unprotected discovery should be used to find

and enroll new members into the NAN Security Group and subsequent protected discovery uses the associated Secure Service ID.

The Secure Service ID is formed as a hash function of the Service Name and the NAN Group Key. This Secure Service ID is then used for all Publish and Subscribe functions for the services protected by the NAN Security Group. The calculation of the Secure Service ID includes high order bits of the NAN TSF and changes periodically.

Secure Service ID = HMAC-SHA-256 (NAN Group Key, Service Name || (TSF & 0xFFFFFFFFFF800000))

Where || represents a concatenation.

7.3 Frame Protection

7.3.1 NDP unicast data frame encryption

A protected NDP uses IEEE 802.11 WPA2 based frame encryption to provide confidentiality and integrity services. The ND-TK for the link encryption is derived using the mechanism specified by the cipher suite selected for the Data Path Setup. Replay detection for protected frames is provided for an NDP and uses the number of replay counters advertised by NDP peer in the Cipher Suite Info NAN attribute.

7.3.2 Management frame protection

This clause describes Management frame protection that applies to all management frames except Beacon frames for which applicable protection is described in section 7.3.4 (Beacon integrity protection).

Unicast management frames related to a given local NMI address are protected using an available NM-TKSA (referring to section 7.6.4.2). Unicast management frames related to a given local NDI address are protected using an available ND-TKSA (referring to section 7.1.3.1).

IGTKSA is primarily used to provide integrity protection for multicast management frames. If an IGTKSA is available, multicast management frames related to a given local NMI address shall be protected using the SA.

Only a single key is used to protect a frame, e.g., when a frame is protected using the NM-TKSA, it is not further protected by the IGTKSA even if one exists.

If a SA is selected to protect a management frame, the key and the cipher (e.g., AES-CCMP-128, BIP-CMAC-128) corresponding to the transmit key ID from the SA is used.

All SDFs between the devices whether or not protected are sent using respective NMI addresses.

Unicast NAN Action Frames shall be sent by using the NMI addresses if the NM-TKSA exists. Otherwise, if an ND-TKSA exists, they may be sent by using the NDI addresses associated with the ND-TKSA.

When IGTKSA is used, the integrity MIC shall be carried in an 802.11 Management MIC element (MME) that appears immediately before the frame FCS field. The encapsulation used shall be as defined in section 11.12 (Group addressed management frame protection procedures) of [1].

NOTE: MME is not a NAN attribute and is not carried in a NAN Element Container attribute.

FTM frames (non-NAN management frames) are not protected.

7.3.3 Group addressed data frame encryption

After a device creates a GTKSA for transmit, for a given local NDI MAC address, it shall protect all group addressed data frames transmitted with that address using the key and the cipher (e.g., AES-CCMP-128) corresponding to the transmit key ID for the SA.

After a device creates a GTKSA for receive, it shall verify protected group addressed frames from the corresponding transmitter. Frames failing verification shall be silently discarded.

7.3.4 Beacon integrity protection

After a device creates a BIGTKSA for transmit, for a given local NMI MAC address, it shall protect all Beacon frames transmitted with that address using the key and the cipher (e.g., BIP-CMAC-128) corresponding to the transmit key ID for the SA.

After a device creates a BIGTKSA for receive, it shall verify protected Beacon frames from the corresponding transmitter. Beacon frames failing verification shall be silently discarded.

In a protected Beacon, the integrity MIC shall be carried in an 802.11 Management MIC element (MME) that appears immediately before the frame FCS field. The encapsulation used shall be as defined in section 11.52 (Beacon frame protection procedures) of [1].

Note: MME is not a NAN attribute and is not carried in a NAN Element Container attribute.

7.4 Security association update

Services requiring NAN unicast data paths between the same local and remote MAC addresses may request security for their corresponding data path. In such a case, the existing SA, if any, shall be updated provided that the new strength of new security is same or greater than the security strength of the existing SA. Otherwise, the existing higher-strength SA will continue to be used after the negotiation and any key material derived for protecting the NDP setup shall be discarded.

Note: If the new strength of new security required by a service is lower than the existing SA, a NDP can be established for the service without an ND-TKSA (referring to section 6.2.1).

For example, if service B requests NCS-SK-128 cipher suite when a unicast NDP initiated by Service A with no security is present, the security association between NDI pairs can be updated to NCS-SK-128 security. This applies to security associations that protect data traffic as well as those that protect management traffic. The new SA applies on the NDP responder once the Security Key install NDP message is sent from the NDP Initiator and is acknowledged by the NDP responder i.e., 802.11 ACK is received for the message. The new security association also applies on the NDP initiator once the Key Install message is acknowledged.

The packet number (PN) shall be set to zero when the new security association applies.

For the purpose of determining security strength, the following strength ordering shall be used (from the highest strength to the lowest strength):

- CSID 8 (NCS-PK-PASN-256) using a password or CSID 4 NCS-PK-2WDH-256
- CSID 7 (NCS-PK-PASN-128) using a password or CSID 3 NCS-PK-2WDH-128
- CSID 2 (NCS-SK-256) using a PSK/Passphrase
- CSID 1 (NCS-SK-128) using a PSK/Passphrase
- CSID 8 (NCS-PK-PASN-256) using opportunistic bootstrapping
- CSID 7 (NCS-PK-PASN-128) using opportunistic bootstrapping
- No security

The NAN Device shall set bit 1 Extended Key ID to zero in the Capabilities field of the Device Capability attribute to indicate that the device does not support pairwise security association update using IEEE 802.11 extended key ID mechanism (refer to [1] section 9.4.2.25.4) and thus there can be data loss during the update.

When an NDP is terminated, the SA in use is not necessarily deleted. If another NDP that required a lower or equal strength security than that provided by the SA, it will continue using the SA provided the lifetime of the SA is not reached. The lifetime of an SA is implementation dependent but can be conveyed to an NDP peer using the NAN Key Lifetime KDE defined in Figure 62.

A NAN Device shall delete the SA when all the NDPs using the SA are terminated.

A NAN Device may update its GTK, IGTK, or BIGTK by using a protected follow-up message. The follow-up message shall include a NAN Shared Key Descriptor attribute with a GTK KDE, IGTK KDE, or BIGTK KDE. The follow-up message may also convey the lifetime of the updated key by including a NAN Key Lifetime KDE in the NAN Shared Key Descriptor attribute.

NOTE: When a NAN Device uses a protected follow-up message to convey a new GTK, it needs to include both a GTK KDE and a MAC address KDE. The MAC address KDE includes the NDI address associated with the GTK.

7.5 NAN discovery security

NAN Synchronization is based on broadcast NAN Synchronization Beacon frames that may be subject to attacks that would disrupt the discovery process. NAN Synchronization Beacon frames could be sent with incorrect TSF timer values or other incorrect information for a cluster that would temporarily change the window timing of nearby devices. The NAN Synchronization process is robust enough to recover from individual malicious frames. It would be possible to continuously disrupt the discovery process by malicious devices continually sending maliciously constructed NAN Synchronization Beacon frames. While a threat, this type of denial of service could just as easily be performed by jamming the channel. This specification does not include mechanisms to mitigate any attacks on the synchronization of a NAN network. Devices implementing NAN Synchronization may implement mechanisms to ignore particular devices or TSF timer values that are clearly incorrect. Such protective behavior is local to device implementations and is not in the scope of this specification.

Service information is carried in unencrypted frames which can be read by passive observers. Sensitive information, such as usernames and addresses, should not be included in unencrypted frames. A service may also be published for a long period of time or it may be published at regular intervals (e.g. user goes to the same coffee shop every morning). Any data that is relatively unique and unchanging, such as MAC addresses, UUIDs, and even dynamic TCP port numbers (since they can act as a 16-bit tracking identifier), may be used to track a user and should not be included in unencrypted frames. When relatively unique data is needed, it should be changed at regular intervals. The recommended change interval is 15 minutes.

The discovery process is inherently based on open communications with newly discovered devices. There may be applications that wish to provide additional privacy and confidentiality of information carried in the NAN Service Discovery frames. Groups can be defined that use the NAN Publish and Subscribe services with additional security built into the application to limit the disclosure of device identities, the services being queried and the contents of the responses.

Devices with fixed MAC addresses can be detected and tracked. The tracking can correlate location information and other behaviors to accurately identify the user, the user’s friends and his favorite applications. NAN provides some privacy by the support of local NAN Interface Addresses. These addresses can be changed occasionally to provide privacy protection against this type of address tracking. The means and frequency of these address changes are local to an implementation, but NMI address of NAN Device shall not change when there is a unicast NDP active on the NAN Device.

The Interface Identifier in the IPv6 Link Local TLV should be generated according to rules specified in RFC 7217 [10].

7.6 NAN pairing

The NAN pairing protocols enable a pair of NAN Devices to authenticate each other when they establish the first trust and verify each other's identity after they set up a pairing relationship. The NAN pairing protocols include a NAN pairing setup protocol and a NAN pairing verification protocol.

7.6.1 NAN pairing primitives

7.6.1.1 Pairing Request method

PairingRequest(type, self_handle, responder_nan_address, paired_peer_handle, pairing_setup_parameters)

Parameters of the PairingRequest method are:

- type
  - pairing setup
  - pairing verification
- self_handle
  - handle of the pairing initiator
- responder_nan_address

  - the pairing responder's NMI
- paired_peer_handle (optional)
  - handle of the paired peer, if type = pairing verification
- pairing_setup_parameters
  - authentication methods
    - password
    - opportunistic
  - NPK/NIK caching
    - Zero if the NPK/NIK caching is disabled
    - One if the NPK/NIK caching is enabled

7.6.1.2 Pairing Response method

PairingResponse(type, status, self_handle, initiator_nan_address, paired_peer_handle, pairing_setup_parameters)

Parameters of the PairingResponse method are:

- type
  - pairing setup
  - pairing verification
- self_handle
  - handle of the pairing responder
- status
  - Decision (Accepted/Rejected)
  - Reason Code
- initiator_nan_address
  - the pairing initiator's NMI
- paired_peer_handle (optional)
  - handle of the paired peer, if type = pairing verification
- pairing_setup_parameters
  - authentication methods
    - password
    - opportunistic
  - NPK/NIK caching
    - Zero if the NPK/NIK caching is disabled
    - One if the NPK/NIK caching is enabled

7.6.1.3 Pairing Indication event

PairingIndication(type, self_handle, initiator_nan_address, responder_nan_address, paired_peer_handle, pairing_setup_parameters)

Parameters of the PairingIndication event are:

- type

  - pairing setup or pairing verification
- self_handle
  - handle of the pairing responder
- initiator_nan_address
  - the pairing initiator's NMI
- responder_nan_address
  - the pairing responder's NMI
- paired_peer_handle (optional)
  - handle of the paired peer, if type = pairing verification
- pairing_setup_parameters
  - authentication methods
    - password
    - opportunistic
  - NPK/NIK caching
    - Zero if the NPK/NIK caching is disabled
    - One if the NPK/NIK caching is enabled

7.6.1.4 Pairing Confirm event

PairingConfirm(type, status, self_handle, initiator_nan_address, responder_nan_address, paired_peer_handle, pairing_setup_parameters)

Parameters of the PairingConfirm event are:

- type
  - pairing setup or pairing verification
- status
  - Decision (Accepted/Rejected)
  - Reason Code
- self_handle
  - handle of the NAN Device, which can be either a pairing initiator or pairing responder
- initiator_nan_address
  - the pairing initiator's NMI
- responder_nan_address
  - the pairing responder's NMI
- paired_peer_handle (optional)
  - handle of the paired peer, if type = pairing verification
- pairing_setup_parameters
  - authentication methods
    - password
    - opportunistic

- NPK/NIK caching
  - Zero if the NPK/NIK caching is disabled
  - One if the NPK/NIK caching is enabled

7.6.2 Pairing identity

A pairing capable device may reveal its long-term identity to paired peers, by including a NIRA in the NAN publish or subscribe messages. The format of the NIRA is defined in section 9.5.21.6.

To produce the NIRA, the device shall generate a NAN Identity Key (NIK), associated with a NIK lifetime. The device shall select the NIK as a random value each time it is generated.

In the NIRA, the value of the Cipher Version indicates the cryptographic parameters and method used to derive the NIR Tag. The NIR cryptographic parameters and methods are defined in Table 22.

Table 22. NIRA Cryptographic Parameters and Methods

Cipher Version	NIK (bits)	Nonce Size (bits)	Tag Size (bits)	Tag Calculation Method
0	128	64	64	Tag = Truncate-64(HMAC-SHA-256(NIK, “NIR”, NMI || Nonce))
1-255	Reserved			

A NAN Device shall provision its NIK to a peer through a secured channel, after it sets up the NAN pairing with the peer. Once the peer obtains the device's NIK, it can correctly identify the device by resolving the NIR Tag included in the received NIRA.

Note: When a NAN Device receives a NIRA from another NAN Device, it derives a set of Tag values based on the cached NIKs of all paired peers. If a derived Tag value matches the Tag value in the received NIRA, the NAN Device identifies the transmitter of the NIRA as a paired peer.

A NAN Device should periodically change its NMI and the Nonce value in the transmitted NIRA, to avoid being tracked by these fields. The recommended change interval is 15 minutes. A NAN Device shall not change its NMI address when it has any active NM-TKSA, ND-TKSA, or NDP.

7.6.3 Pairing capability and operation indications

A NAN Device uses the following information fields and attributes to indicate its pairing capabilities and operation modes:

- CSIA
  - NCS-PK-PASN-128 or NCS-PK-PASN-256 Cipher Suite
- DCEA
  - Pairing Setup Enabled bit
  - NPK/NIK Caching Enabled bit
- NAN Identity Resolution (NIR) attribute

Table 23 summarizes the pairing operation modes and indications.

Table 23. Pairing Operations Modes and Indications

Pairing Setup Enabled bit in DCEA	NPK/NIK Caching Enabled bit in DCEA	NIRA	Description
Set to 1	Set to 1	Not Present	A NAN Device enables both the pairing setup and the NPK/NIK caching with unpaired devices. The NAN Device disables the pairing verification with any device.

Pairing Setup Enabled bit in DCEA	NPK/NIK Caching Enabled bit in DCEA	NIRA	Description
Set to 1	Set to 1	Present	A NAN Device enables both the pairing setup and the NPK/NIK caching with unpaired devices. The NAN Device also enables the pairing verification with already paired devices.
Set to 1	Set to 0	Present	A NAN Device enables the pairing setup with unpaired devices but disables the NPK/NIK caching with unpaired devices. The NAN Device enables the pairing verification with already paired devices.
Set to 1	Set to 0	Not Present	A NAN Device enables the pairing setup with unpaired devices but disables the NPK/NIK caching with unpaired devices. The NAN Device disables the pairing verification with any device.
Set to 0	Reserved	Present	A NAN Device disables the pairing setup with unpaired devices. The NAN Device enables the pairing verification with already paired devices.
Other combinations			Reserved

7.6.4 Pairing setup

A NAN Device which enables the NAN pairing setup indicates its pairing capabilities and operations in publish or subscribe messages, according to section 7.6.3.

7.6.4.1 Pairing bootstrapping

The NAN pairing setup typically needs an OOB bootstrapping to enable a bootstrapping initiator and a bootstrapping responder to possess a same pairing credential.

A NAN Device which enables the NAN pairing setup indicates its pairing bootstrapping capabilities by including a NPBA in publish or subscribe messages:

- The Type subfield of the NPBA is set to 0 (Advertise)
- The Pairing Bootstrapping Method field indicates at least one supported pairing bootstrapping methods

A bootstrapping initiator starts the pairing bootstrapping by transmitting a follow-up message to a bootstrapping responder. The follow-up message shall include a NPBA. The Type subfield of the NPBA shall be set to 1 (Request), and the Pairing Bootstrapping Method field shall indicate one selected pairing bootstrapping method, which shall match with a pairing bootstrapping method supported by the bootstrapping responder. For example, if a bootstrapping responder indicates that it supports pin-code display and QR-code display, the bootstrapping initiator shall select from one of the matched methods: keypad (pin-code only), keypad (passphrase), or QR-code scan.

When the bootstrapping responder receives a follow-up message with a bootstrapping request from the bootstrapping initiator, it shall transmit a follow-up message back. The follow-up message shall include a NPBA. The Type subfield of the NPBA is set to 2 (Response), and the Status subfield is set to 0 (Accepted) or 1 (Rejected). If the bootstrapping request is accepted, the Pairing Bootstrapping Method field shall indicate a method matched with the selected method from the bootstrapping initiator; otherwise, the Pairing Bootstrapping Method field value shall be ignored, and the Reason Code field shall indicate a rejection reason.

If a bootstrapping responder needs to spend considerable amount of time to process a bootstrapping request, it may respond a follow-up message with a comeback request. The follow-up message shall include a NPBA with following fields and settings:

- The Type subfield is set to 2 (Response)
- The Status subfield is set to 2 (Comeback)

- The Comeback After subfield of the Comeback field is set to the deferral time the bootstrapping initiator is expected to resend the bootstrapping request
- The Cookie is optionally present in the Comeback field, and is an opaque sequence of octets generated and validated by the bootstrapping responder by an implementation dependent scheme
- The Pairing Bootstrapping Method field value shall be ignored

When a bootstrapping initiator receives a bootstrapping response with a comeback request, it shall resend the bootstrapping request after the deferral time indicated by the value of the Comeback After subfield in the Comeback field of the received follow-up message. If the Comeback field of the received follow-up message also includes a Cookie, the bootstrapping initiator shall resend the bootstrapping request, which includes a NPBA with following fields and settings:

- The Type subfield is set to 1 (Request)
- The Status subfield is set to 2 (Comeback)
- The Comeback field is presented with the same Cookie received from the bootstrapping responder

After the follow-up message handshakes, if the bootstrapping responder accepts the bootstrapping request, the bootstrapping responder and the bootstrapping initiator shall execute the selected pairing bootstrapping method and acquire a common pairing credential.

Figure 46 shows an example of the pairing bootstrapping handshakes. In the example, the bootstrapping initiator and the bootstrapping responder are a service subscriber and a service publisher respectively.

Table 24 summarizes the paring bootstrapping methods conveyed by the NPBA.

Table 24. Pairing Bootstrapping Methods

Pairing Bootstrapping Methods	Description
Opportunistic bootstrapping	A pairing peer with simple user interface may rely on pushbutton or other OOB means to bootstrap the pairing setup without mutual authentication (referring to section 7.6.4.3).
Pin-code display	Device is capable of display a pin-code (4 digits or more).
Passphrase display	Device is capable of display a passphrase (8 - 63 ASCII-encoded characters).
QR-code display	Device is capable of display a QR-code represented by the WIFI URI [21].
NFC Tag	Device is capable of supporting the NFC Tag.
Keypad (pin-code only)	Device is capable of entering a pin.
Keypad (passphrase)	Device is capable of entering a passphrase
QR-code scan	Device is capable of scan a QR-code represented by the WIFI URI [20].
NFC reader	Device is capable of supporting the NFC reader.
Service managed bootstrapping	The bootstrapping is entirely managed and executed by the service/application and is transparent to the NAN engine. The service may use the service info field of the SDEA to convey bootstrapping configuration information through the subscribe, publish, and bootstrapping follow-up messages.
Bootstrapping handshakes skipped	Device acquires the pairing credential by means out of scope of this specification and does not need the pairing bootstrapping handshakes.

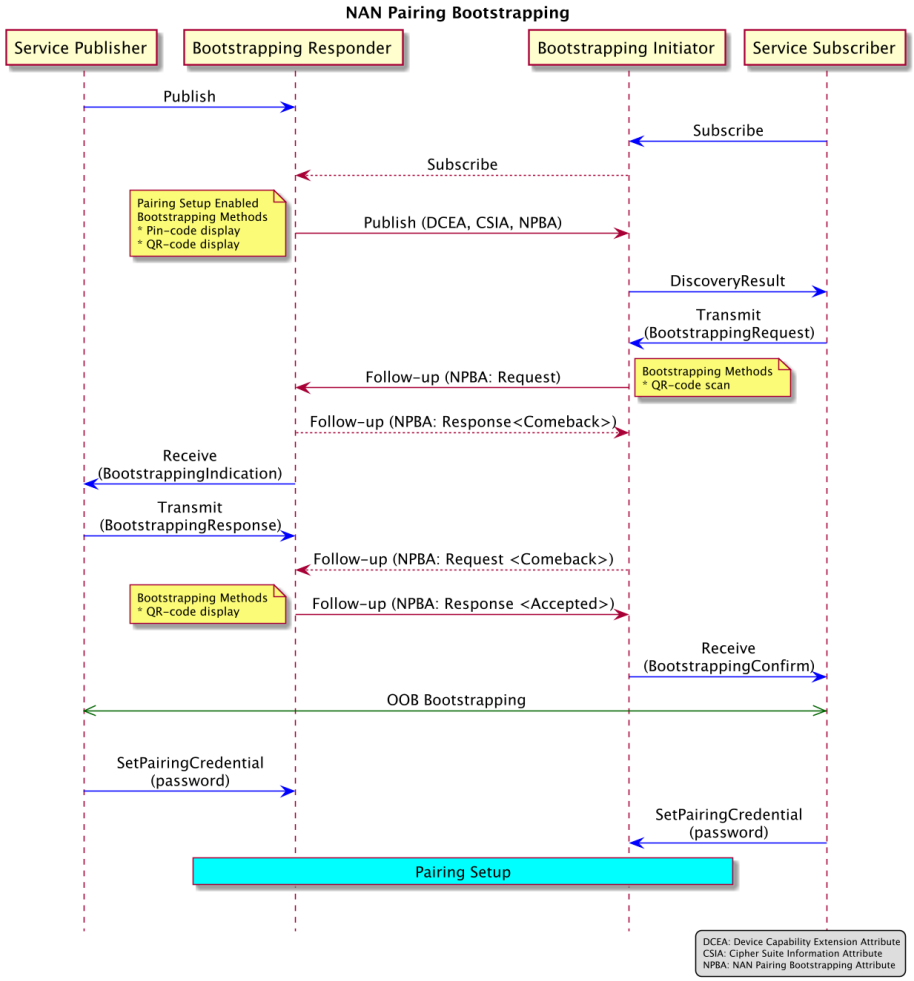


Figure 46. Example of NAN pairing bootstrapping

7.6.4.2 Pairing setup using a password

Most pairing bootstrapping methods enable a pairing peer to possess a common password.

A pairing initiator may initiate the pairing setup with a pairing responder and authenticate each other by proving possession of a password.

The password-authenticated pairing setup employs the PASN authentication with SAE tunneling, as defined in section 12.12.5 of [20]. The PASN Authentication frames are used in the pairing setup handshakes, with the base AKM set as SAE and the NPK/NIK caching (equivalent to PMK caching in [19]) not used.

The SSID used in SAE shall be set to the string "516F9A010000".

The first PASN Authentication frame is transmitted by the pairing initiator and shall include the contents as defined in section 12.12.5 of [20], as well as a NAN IE with following NAN attributes:

- A DCEA with the Pairing Setup Enabled bit set to 1 and the NPK/NIK Caching Enabled bit set to 1 or 0, according to the corresponding indication advertised by the pairing responder
- A CSIA, indicating the selected NCS-PK-PASN cipher suite for the pairing setup, which shall be the best NCS-PK-PASN cipher suite supported by both peers
- An NPBA, which shall be the same as that included in the pairing bootstrapping request follow-up message from the pairing initiator, if the pairing bootstrapping handshakes were conducted successfully before the pairing setup

The second PASN Authentication frame is transmitted by the pairing responder and shall include the contents as defined in section 12.12.5 of [20], as well as a NAN IE with following attributes, which shall be the same as those included in the publish or subscribe messages transmitted by the pairing responder:

- A DCEA
- A CSIA
- An NPBA

The third PASN Authentication frame is transmitted by the pairing initiator and shall include the contents as defined in section 12.12.5 of [20].

The RSNE and the RSNXE in the first and second PASN Authentication frames shall be set according to Table 25 and Table 26, respectively.

The RSNE and the RSNXE included in the second PASN Authentication frame shall be used as the "Beacon RSNE" and the "Beacon RSNXE" in the MIC computation for the second PASN Authentication frame (referring to section 12.12.8.1 of [20]).

The pairing responder's NMI and the pairing initiator's NMI are used to replace "BSSID" and "SPA" in key and MIC calculations.

Table 25. RSNE Settings in PASN Authentication Frames

	Version	Group Data Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKID Count	PMKID List	Group Management Cipher Suite
First PASN frame	1	00-0F-AC-7 (Not Allowed)	1	One or more of CCMP-128 and GCMP-256	1	SAE	MFPC=1 MFPR=1	0	Empty	00-0F-AC-7 (Not Allowed)
Second PASN frame	1	00-0F-AC-7 (Not Allowed)	1	CCMP-128 or GCMP-246	1	SAE	MFPC=1 MFPR=1	1	NPKID*	00-0F-AC-7 (Not Allowed)

Table 26. RSNXE Settings in PASN Authentication Frames

	Extended RSN Capabilities									
	b0-b3	b4	b5	b6	b7	b8	b9	b10	b11	b12-b15
	Field Length	Protected TWT Operations Support	SAE hash-to-element	Reserved	Protected WUR Frame Support	Secure LTF Support	Secure RTT Supported	URNM-MFPR	Protected Announce Support	Reserved
First PASN frame	1	Reserved	1	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
Second PASN frame	1	Reserved	1	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

*__NOTE:__ The NPKID included in the RSNE of the second PASN frame is set to the PMKID generated by SAE.

Note: A pairing initiator or pairing responder can include a NAN Availability attribute in the NAN IE of the PASN Authentication frames to indicate updated NAN availability schedules.

Figure 47 shows an example of the pairing setup using a password. In the example, the pairing initiator and the pairing responder are a service subscriber and a service publisher respectively.

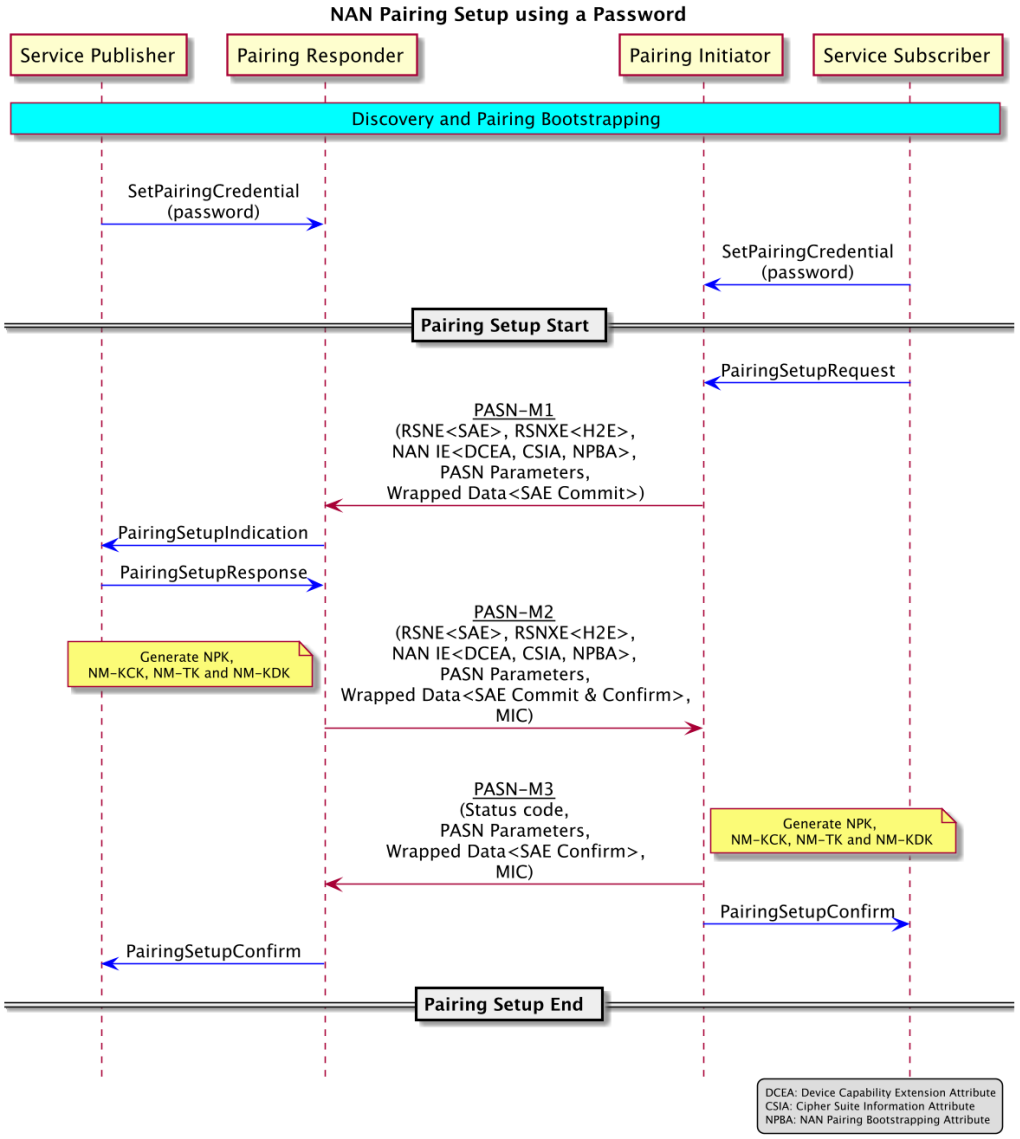


Figure 47. Example of NAN pairing setup using a password

A NPKSA is established between the pairing initiator and the pairing responder after the successful completion of the pairing setup.

The NPKSA is equivalent to the PMKSA, as defined in section 12.6.1.1.2 of [1], and contains:

- A NPKID (equivalent to PMKID). The NPKID identifies the security association
- The local NIK and the peer's NIK, if the NPK/NIK caching is enabled
- A base AKM (SAE or PASN Opportunistic Pairing) used to establish the security association
- A cipher suite agreed upon and identified by a CSID
- A shared symmetric key (NPK), which is equivalent to PMK in [1] and [20]
- Lifetime

A NM-TKSA is derived from the NPK of the NPKSA, in the same way as the PTKSA derivation with PASN authentication, as described in section 12.12.7 of [20]. The key derivation is as follows:

NM-KCK || NM-TK || NM-KDK = KDF-HASH-NNN (NPK, “PASN PTK Derivation”, Pairing Initiator NMI || Pairing Responder NMI || DHss)

NNN is the Bits required for generated keys, which is either 640 or 768 depending on the pairwise cipher (referring to 12.12.7 of [20]).

Once the NM-TKSA is established (and the corresponding NM-TK is derived), all subsequent NAN management frame exchanges shall be protected by PMFs using the NM-TK.

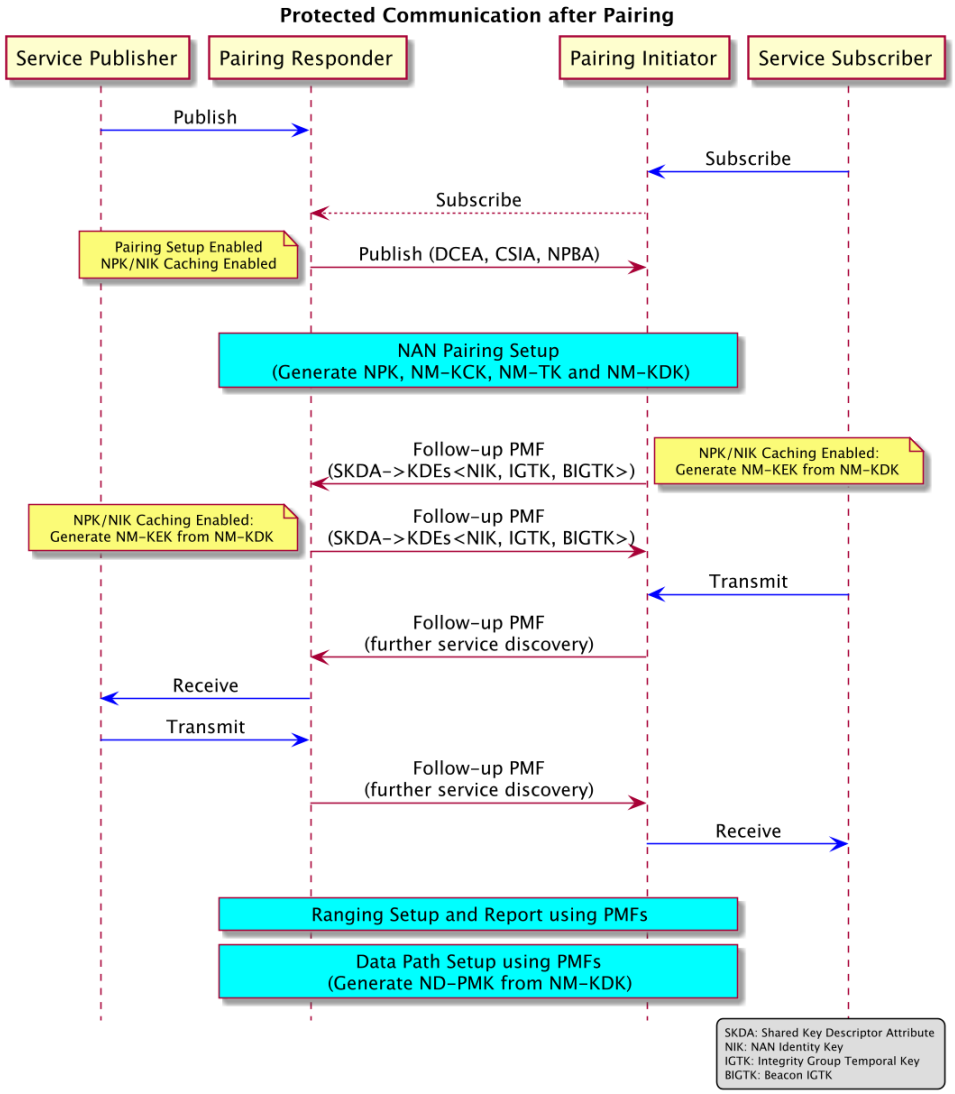


Figure 48. Example of protected communication after pairing

Figure 48 shows an example of protected follow-up, ranging setup, and data path setup after the NAN pairing setup. In the example, the pairing initiator and the pairing responder are a service subscriber and a service publisher respectively.

If a pairing responder enables the NPK/NIK caching, it shall set the NPK/NIK Caching Enabled bit of the DCEA to one (1), which is conveyed by the publish or subscribe messages, as well as the second PASN Authentication frame. The pairing responder shall also generate a NIK as specified in section 7.6.2.

If a pairing initiator starts the pairing setup with a pairing responder and enables the NPK/NIK caching, it shall set the NPK/NIK Caching Enabled bit of the DCEA to one (1), which is conveyed by the first PASN Authentication frame. The pairing initiator shall also generate a NIK.

The pairing initiator shall initiate the NIK exchange with the pairing responder if the pairing setup is completed successfully. The NIK exchange uses the follow-up handshakes, protected by the NM-TK. The follow-up messages from both the pairing initiator and pairing responder shall include a NAN Shared Key Descriptor attribute with a NIK KDE and a NAN Key Lifetime KDE including the NIK's lifetime. The same follow-up messages may also be used to exchange other keys, like BIGTK and IGTK, in which case, the NAN Shared Key Descriptor attribute may also include a BIGTK KDE and a IGTK KDE, as well as corresponding NAN Key Lifetime KDEs.

The Key Data field of the NAN Shared Key Descriptor attribute shall be encrypted by a NM-KEK computed as follows:

NM-KEK = KDF-HASH-MMM (NM-KDK, “NAN Management KEK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)

where MMM is number of bits in NM-KEK. MMM shall be the same as the bit length of the corresponding NM-TK (Unicast Encryption Key).

Once the pairing responder and the pairing initiator receive each other's NIK, they can refer to the cached NPK and the corresponding NPKSA by using <local NIK, peer NIK>.

If a NAN Device, either a pairing initiator or pairing responder, does not enable the NPK/NIK caching, it shall delete the NPK and the corresponding NPKSA once the NM-TKSA is established (and the corresponding NM-TK and NM-KDK are derived).

If a NAN Device enables the NPK/NIK caching with a peer but does not receive the NIK from the peer after the pairing setup, it shall delete the NPK and the corresponding NPKSA after a timeout.

If a pairing initiator and pairing responder establish a secure NDP after a successful pairing setup or pairing verification, they shall derive the ND-PMK for the NDP as:

ND-PMK = KDF-HASH-256 (NM-KDK, “NDP PMK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)

Note: ND-PMK is associated with the Pairing Initiator NMI and the Pairing Responder NMI of a NM-TKSA. A same ND-PMK can be used to establish multiple secured NDPs between a Pairing Initiator and a Pairing Responder.

7.6.4.3 Pairing setup using opportunistic bootstrapping

The opportunistic bootstrapping enables NAN Devices with very simple user interface (for example, a button and a LED) to establish the NAN pairing with other NAN Devices, without providing, acquiring, and proving possession of a pairing credential.

The pairing setup with opportunistic bootstrapping employs the unauthenticated PASN, as specified in section 12.12.3.2 of [20]. The pairing setup handshakes also use the PASN Authentication frames, but with the base AKM set as the PASN AKM.

The PASN Authentication frames shall include the contents as defined in section 12.12.3.2 of [20]. In addition, the first and second PASN Authentication frames shall also include a NAN IE with corresponding NAN attributes, as specified in section 7.6.4.2 (for the pairing setup using a password).

The RSNE in the first and second PASN Authentication frames shall be set according to Table 25 and Table 26, except that:

- In both frames, the AKM suite shall be set to PASN AKM instead of SAE
- In both frames, the PMKID count shall be set to 0

If the RSNXE is present in the PASN Authentication frames, the value of the SAE hash-to element field is ignored.

After the successful completion of the pairing setup, a NPKSA is established between the pairing initiator and the pairing responder, and a NM-TKSA is derived from a NPK set to the string "PMKz" padded with 28 0s (as defined in section 12.12.7 of [20]). The key derivations and key usages are the same as those specified in section 7.6.4.2 (pairing setup using a password).

If the pairing responder and the pairing initiator enable the NPK/NIK caching, they shall also derive a cached NPK as follows:

NPK = KDF-HASH-256(NM-KDK, “NAN Opportunistic NPK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)

Figure 49 shows an example of the pairing setup using opportunistic bootstrapping. In the example, the pairing initiator and the pairing responder are a service subscriber and a service publisher respectively.

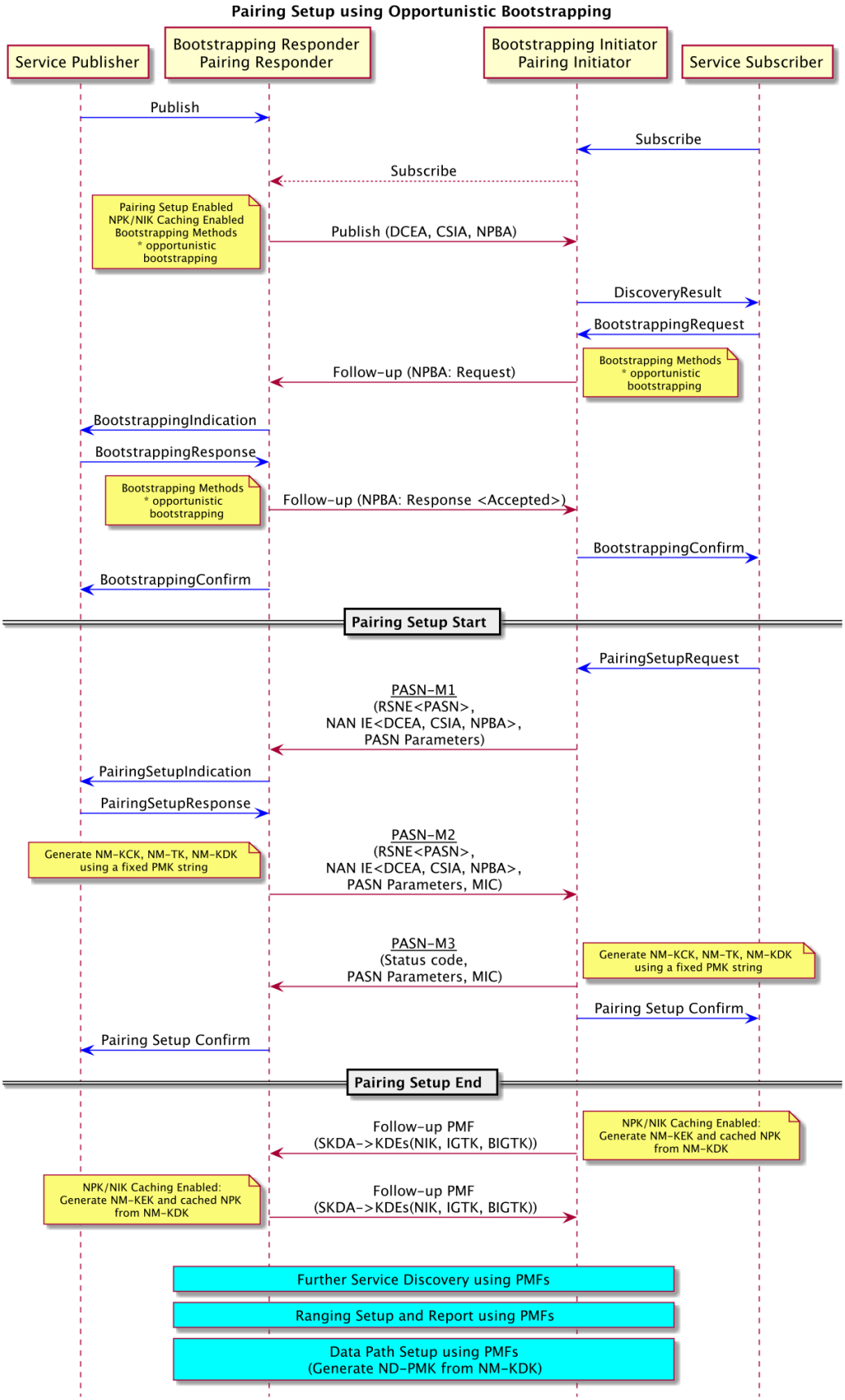


Figure 49. Example of pairing setup using opportunistic bootstrapping

7.6.5 Pairing verification

The NPK/NIK caching allows a NAN Device pair to identify each other based on the cached NIKs and authenticate each other based on the cached NPK. So that the device pair can reconnect autonomously, without enduring the pairing bootstrapping and the pairing setup again.

A NAN Device which enables the NAN pairing verification shall include a NIRA in publish or subscribe messages. A peer device which are interested in connecting to the NAN Device may resolve the Tag in the NIRA (as described in section 7.6.2 and identify whether the NAN Device is a paired peer.

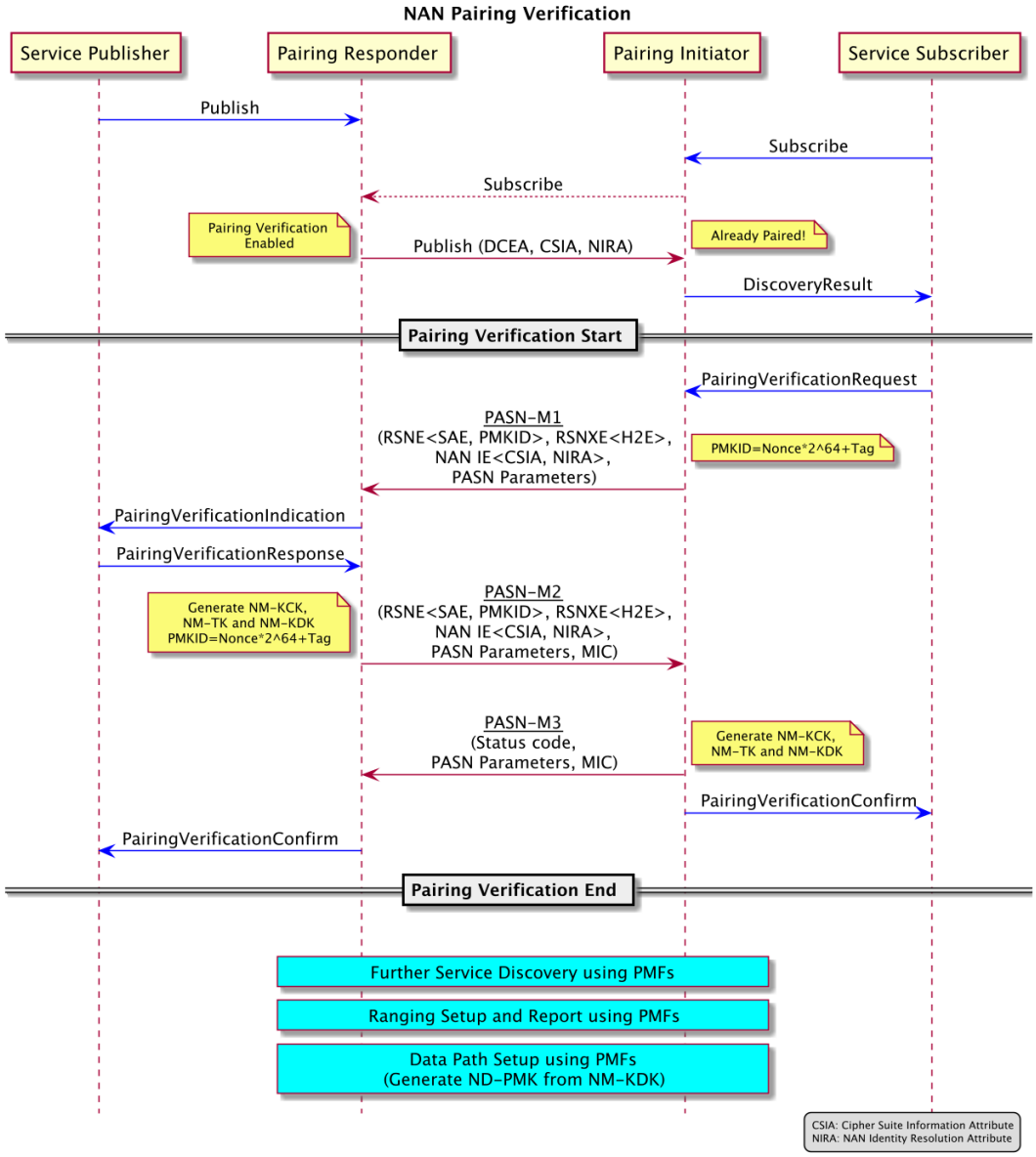


Figure 50. Example of NAN pairing verification

A pairing initiator may initiate the pairing verification with a pairing responder, if:

- The pairing initiator identifies the pairing responder as a paired peer, and
- The pairing initiator maintains a cached NPKSA with the pairing responder

The pairing verification employs the PASN authentication with the NPK caching (equivalent to the PMK caching) as defined in section 12.12.3.2 of [20]. The pairing verification handshakes use the PASN Authentication frames, with the base AKM set as the AKM associated with the cached NPKSA.

The first PASN Authentication frame shall include the contents as defined in section 12.12.3.2 of [20], as well as a NAN IE with following NAN attributes:

- A CSIA
- A NIRA

The second PASN Authentication frame shall include the contents as defined in section 12.12.3.2 of [20], as well as a NAN IE with following attributes, which shall be the same as those included in the publish or subscribe messages transmitted by the pairing responder:

- A CSIA
- A NIRA

The third PASN Authentication frame shall include the contents as defined in section 12.12.3.2 of [20].

NOTE: A pairing initiator or pairing responder can include a NAN Availability attribute in the NAN IE of the PASN Authentication frames to indicate updated NAN availability schedules.

The RSNE and the RSNXE in the first and second PASN Authentication frames shall be set according to Table 25 and Table 26, except that:

- In both frames, the AKM suite in the RSNE shall be set to the AKM associated with the cached NPKSA
- In both frames, the PMKID count in the RSNE shall be set to 1 (one), and the 16-byte PMKID shall be set to: PMKID = Tag *2^64 + Nonce (i.e. Tag is MSB and Nonce is LSB), where the Nonce and Tag are values copied from the Nonce and Tag fields of the NIRA included in the same PASN Authentication frame
- If the AKM associated with the cached NPKSA is SAE, the SAE hash-to-element field in the RSNXE shall be set to one; otherwise, the value of the SAE hash-to-element field is ignored

NOTE: A NAN Device pair with a cached NPKSA shall not include the NPKID in any unencrypted frames, except for the second PASN Authentication frame in the pairing setup using a password, as shown in Table 25.

Figure 50 shows an example of the pairing verification using the NPK/NIK caching. In the example, the pairing initiator and the pairing responder are a service subscriber and a service publisher respectively.

If the pairing verification is completed successfully, a NM-TKSA is derived from the cached NPK. The key derivation and key usages are the same as those specified in section 7.6.4.2 (pairing setup using a password).

7.6.6 Pairing key relationships

Figure 51 illustrate the relationships between the NAN pairing, verification, key distribution, and NDP setup operations, as well as the keys derived during these operations.

Table 27 summarizes the NAN key usages.

Table 27. NAN Key Usages

Key Name	Key Usage
NIK	A random value, assigned by a device, that is used to enable a paired peer to resolve the identity of the device based on the NIRA received from the device
NPK	A master pairing key used to derive the temporal keys of a NM-TKSA, which is established after either the pairing setup or pairing verification
NM-KCK	A key confirmation key used to provide data origin authenticity in the PASN authentication frames
NM-TK	A transient key used to protect the NMI addressed unicast NAN management frames, including Follow-up SDFs, as well as Ranging, Data Path Setup, and Schedule NAFs
NM-KDK	A key derivation key used to derive • NPK (for opportunistic pairing) • NM-KEK (for KDE encryption) • ND-PMK (for setting up a secured NAN Data Path)
NM-KEK	A key encryption key for protecting the Key Data field of the NAN Shared Key Descriptor attribute included in the SDFs

Key Name	Key Usage
IGTK	A random value, assigned by a device, that is used to provide integrity protection for the NMI addressed multicast management frames from the device
BIGTK	A random value, assigned by a device, that is used to provide integrity protection for the NAN Beacon frames from the device
ND-PMK	A pairwise master key used to derive the temporal keys of a ND-TKSA, which is established after a successful secured NDP setup
ND-KCK	A key confirmation key used to provide data origin authenticity in the Data Path Setup NAFs
ND-KEK	A key encryption key for protecting the Key Data field of the NAN Shared Key Descriptor attribute included in the Data Path Setup NAFs
ND-TK	A transient key used to protect the NDI addressed unicast data frames and management frames, such as the Data Path Termination frame
GTK	A random value, assigned by a device, that is used to protect the NDI addressed multicast data and management frames from the device

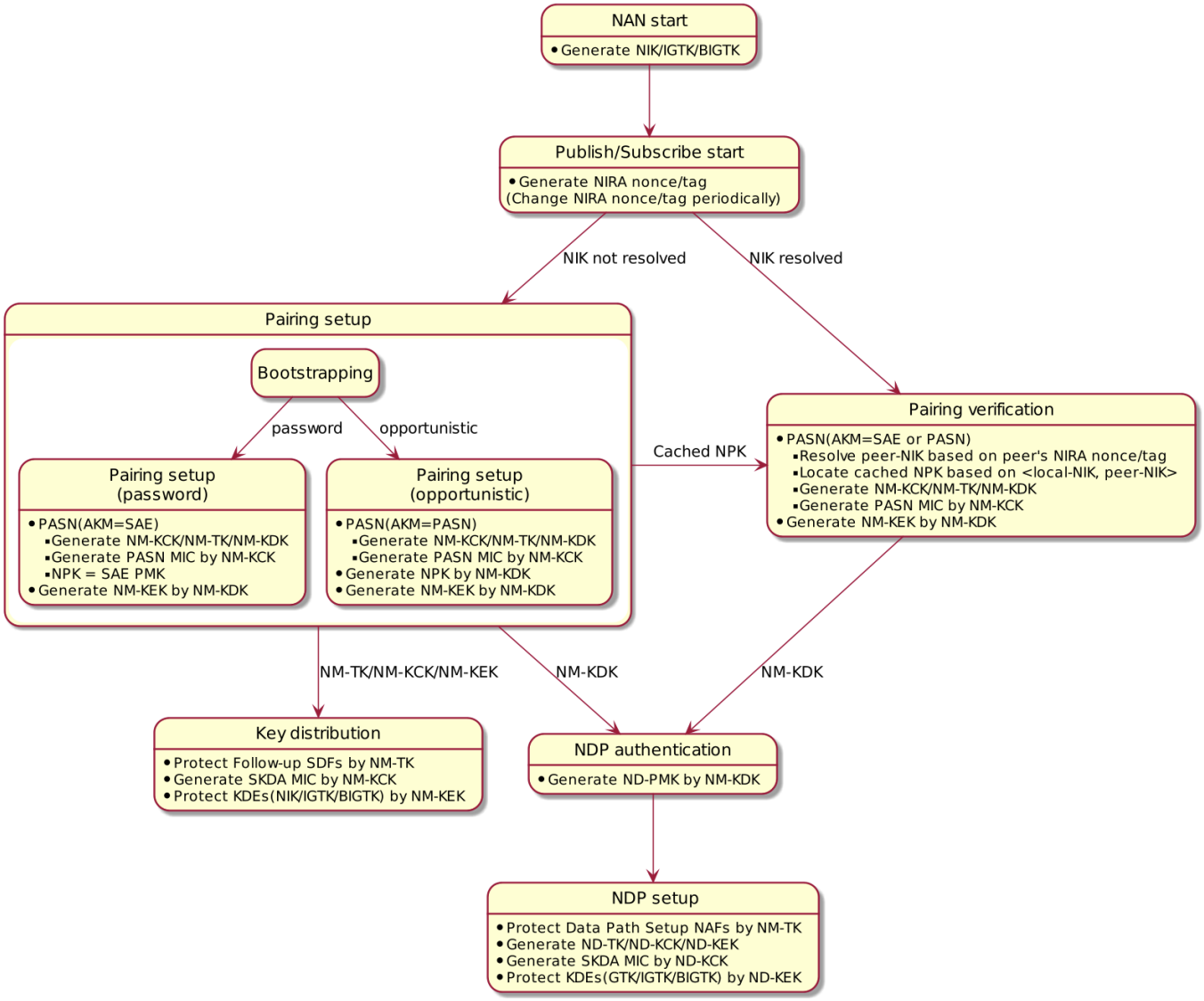


Figure 51. NAN pairing operations and key relationship

The NM-TK is associated to the NMI addresses of the device pair, therefore, if a unicast NAN management frame uses the NMI addresses in A1 and A2, it shall be protected by the NM-TK.

The ND-TK is associated to the NDI addresses of the device pair, therefore, if a unicast NAN management frame uses the NDI addresses in A1 and A2, it shall be protected by the ND-TK.

If both devices of a device pair use the NMIs as their NDIs, the strongest and latest TK is used to protect the unicast NAN management and data frames (referring to section 7.4).

Table 28 summarizes NAN key and key identifier derivations.

Table 28. NAN Key and Key Identifier Derivation Summary

	NCS-SK (CSID = 1 or 2)	**NCS-PK-PASN (CSID = 7 or 8)**
NPK	N/A	NAN Pairing Setup • using a password: NPK is derived by SAE • opportunistic: NPK = KDF-HASH-256(NM-KDK, “NAN Opportunistic NPK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)
NPK Identifier	N/A	NAN Pairing Setup using a password: • PMKID in PASN M2: derived by SAE NAN Pairing Verification: • PMKID in PASN M1 and M2: PMKID = Tag *2^64 + Nonce
NM-TKSA keys	N/A	NM-KCK || NM-TK || NM-KDK = KDF-HASH-NNN (NPK, “PASN PTK Derivation”, Pairing Initiator NMI || Pairing Responder NMI || DHss) NM-KEK = KDF-HASH-MMM (NM-KDK, “NAN Management KEK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)
ND-PMK	ND-PMK = PBKDF2(<pass phrase>, <Salt Version>||<Cipher Suite ID>||<Service ID>||<Publisher NMI>, 4096, 32)	ND-PMK = KDF-HASH-256 (NM-KDK, “NDP PMK Derivation”, Pairing Initiator NMI || Pairing Responder NMI)
ND-PMK Identifier	ND-PMKID in Secured Data Path Setup (M1, M2) • ND-PMKID = L(HMAC-Hash (ND-PMK, “NAN PMK Name” || NDP Initiator NMI || NDP Responder NMI || Service ID), 0, 128)	
ND-TKSA keys	ND-KCK || ND-KEK || ND-TK = PRF-Length (ND-PMK, “NAN Pairwise key expansion”, NDP Initiator NDI || NDP Responder NDI || INonce || RNonce)	

8 NAN ranging

8.1 NAN ranging overview

The NAN Ranging component provides means for a service on a NAN Device to initiate range measurement to and/or from other NAN device that supports the NAN ranging capability.

If NAN Ranging is supported, then the NAN Ranging component shall be invoked explicitly for a NAN service as well as a part of a NAN service discovery, as shown in Figure 52.

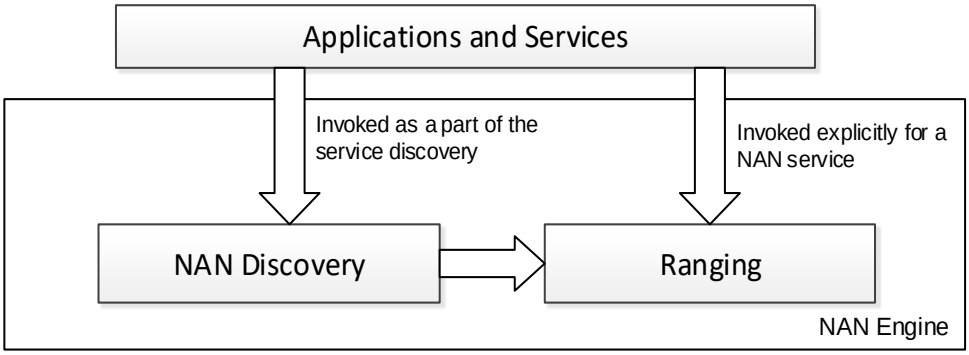


Figure 52. Ranging component initiation

The NAN Ranging component also supports geofencing, which is a virtual perimeter for a real-world geographic area. As a ranging service, NAN geofencing enables the Ranging component (see Figure 7) to trigger an event when a certain range condition is met. See Figure 53 for examples of egress and ingress geofences.

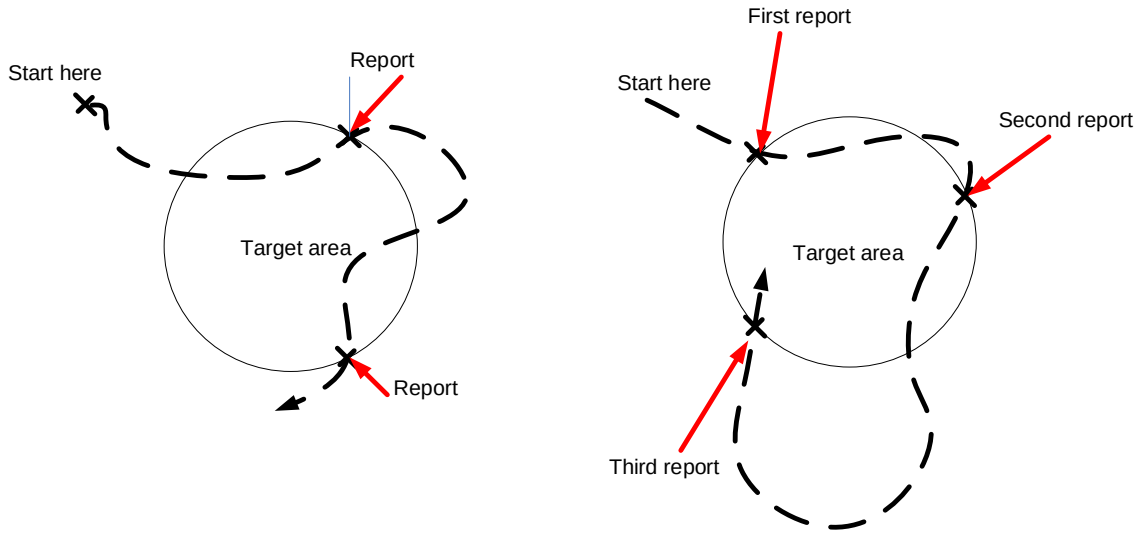


Figure 53. Egress and ingress geofences

The Ranging Info and NAN Availability attributes that are included in the SDF are used to advertise the ranging device's ranging capability and availability for ranging operation.

The Ranging Setup attribute along with the Ranging Info attribute and NAN Availability attribute that are included in the Ranging Request frame and Ranging Response frame are used to negotiate the parameters and schedule for ranging measurement procedure setup.

The fine timing measurement (FTM) procedure, as defined in [1], is used to obtain a NAN device's range to another NAN device, with the following restrictions:

- ASAP = 1
- Number of Burst Exponent = 0 (Single Burst)

8.2 NAN ranging primitives

8.2.1 Methods

Range_Request(MAC_Address, range_id, configuration_parameters)

Parameters of the Range_Request method are:

- MAC_Address
  - MAC address of the NAN device for which the range is to be determined.
- configuration_parameters
  - Ranging resolution

    Determines the accuracy required from the ranging
  - Ranging interval

    The maximum interval between two ranging measurements
  - Ranging indication condition, with following values:

    Continuous (default): When the Ranging indication condition is set to the value of “continuous”, the ranging result will be reported continuously.

    Ingress: When the ranging indication condition is set to the value of “Ingress”, the ranging result will be reported when the device moves into the range of the inner threshold.

    Egress: When ranging the indication condition is set to the value of “Egress”, the ranging result will be reported when the device moves out of the range of the outer threshold.

    both_Ingress_Egress: When the ranging indication condition is set to the value of “both_Ingress_Egress”, the ranging result will be reported when the device moves either into the range of the inner threshold or out of the range of the outer threshold.
  - Geofence description – the range parameters defining the geofence. Valid if ranging indication condition is set to Ingress, Egress or both_Ingress_Egress

    inner threshold: The distance at which the inner threshold is met. Valid if ranging indication condition is Ingress or both_Ingress_Egress.

    outer threshold: The distance at which the outer threshold is met. Valid if ranging indication condition is Egress or both_Ingress_Egress.

The method returns:

- range_id

  A handle uniquely identifying a ranging to be used by the invoker of the ranging component

8.2.1.1 Cancel Ranging method

Cancel_Range(range_id):

Cancels the range request made using the handle range_id.

8.2.1.2 Range Response method

Range_Response(response_control_parameters, matching_filter_for_response, range_id, configuration_parameters)

Parameters of the Range_Response method are:

- response_control_parameters
  - Auto-Response flag

    Set to true to indicate the Ranging Engine can auto response. Otherwise, the Ranging Engine sends a Ranging_Request_Indication event to the service. If the Auto-Response flag is set to true and “matching filter for Response” is present, the Ranging Engine will accept the ranging request if the matching filter is matched. If the Auto-Response flag is set to true and “Matching filter for response” is not present, the NAN engine will accept all ranging requests.
  - Ranging Result flag

    Set to 1 to indicate a Ranging result is required. Otherwise, set to 0.
  - Status

    Set to 1 indicates that the status will be returned from the service. Status will be either Accepted or Rejected (with possible reject reason code). This field is reserved if the Auto-Response flag is set to true.
- matching_filter_for_response
  - Ordered sequence of <length, value> pairs which specify response conditions used to filter ranging request messages for auto-response
- range_id
  - Handle uniquely identifying a ranging request, ranging response, Publish, Subscribe, NDL handle, or service interface handle that called the Ranging component
- configuration_parameters
  - Ranging resolution

    Determines the accuracy required from the ranging
  - Ranging Interval

    The maximum interval between two ranging measurements
  - Ranging indication condition

    See definition in the Range Request Method
  - Geofence description

    See definition in the Range Request Method

8.2.2 Events

8.2.2.1 Range Result event

Range_Result (MAC_Address, range_id, range_measurement, event_type)

Parameters of the Range_Result event are:

- MAC_Address

  MAC address of the device for which the range measurement has been computed
- Range_id

  Uniquely identifying the range request
- range_measurement

  Distance to the NAN device with the MAC address indicated with the MAC_Address parameter

- event_type

  The event type is set to one of the following setting, depending on the value of the ranging indication condition parameter in the Range Request:

  inner threshold met: if the ranging indication condition set to Ingress or both_Ingress_Egress.

  outer threshold met: if the ranging indication condition set to Egress or both_Ingress_Egress.

  Continues: if the ranging indication condition is set to Continues

8.2.2.2 Range Request Indication event

Range_Request_Indication (MAC Address, range_id, configuration_parameters)

Parameters of the Range_Request_Indication event are:

- MAC_Address

  MAC address of the device for which the range is to be determined.

- range_id

  Handle uniquely identifying the range request

- configuration_parameters

  Configuration parameters received from the ranging request in the NAN SDF

8.3 NAN ranging procedure

NAN ranging allows a NAN Device to obtain its range to another NAN Device in the same NAN cluster. The NAN ranging procedure includes:

- NAN ranging capability exchange
- NAN ranging session setup, update, and termination
- NAN ranging report
- FTM protocol and procedure

A NAN ranging session consists of one or more scheduled executions of the fine timing measurement (FTM) procedure between an initiating NAN Ranging device (Ranging Initiator) and a responding NAN Ranging device (Ranging Responder) along with the associated ranging schedule time blocks and operational parameters of that instance.

The ranging schedule is negotiated and established by two devices' NAN Schedulers.

The fine timing measurement procedure that is used in the NAN Ranging is a Single Burst (number of burst exponent=0) and ASAP mode (ASAP=1) procedure, hereafter called a Single Burst ASAP FTM session.

A NAN ranging session is composed of one or more Single Burst ASAP FTM sessions operating at the associated ranging schedule.

On completing the Single Burst ASAP FTM range determination, the device obtains the range result and may send the result to the service.

If an ingress geofence is configured, an event is sent by the NAN Engine to an application registered for the service when the device moves into the range of the inner threshold. If an egress geofence is configured, an event is sent by the Ranging Engine to an application registered for the service when the device moves out of the range of the outer threshold.

A NAN Ranging device might have concurrent NAN Ranging sessions with multiple NAN Ranging device in the NAN cluster.

The NAN Management Interface (NMI) is used for the ranging operation and shall not be changed in the ranging session.

8.3.1 NAN ranging capability exchange

Implementation of the NAN Ranging component is optional for a NAN device. A NAN Device that supports the NAN Ranging component shall support both FTM Initiator and FTM Responder capabilities.

A NAN device that supports the NAN Ranging component shall include the Ranging Information attribute in the SDF frames. If the Ranging Information attribute is included in the SDF frame, one or more NAN Availability attributes shall be included in the SDF frame to indicate potential FAWs for the NAN Ranging operation.

A NAN device shall initiate the ranging setup procedure only with a NAN Device that supports the NAN Ranging component. The Ranging Information attribute shall also be included in the Ranging Request and Ranging Response frames for the ranging setup.

A NAN Ranging device shall indicate whether it has location information availability using the Location Information Availability field in the Ranging Information attribute. A NAN Ranging device may request location information from the device indicating the corresponding location information available by using the FTM Request frame as defined in [1].

An initiating or responding NAN Ranging device may provide the last movement indication in the Ranging Information attribute. The receiving device may use the value of the Last Movement Indication to decide whether a ranging operation is needed, or an existing ranging session need to be updated or terminated.

8.3.2 NAN ranging invoked by a NAN service

The NAN ranging session setup may be initiated explicitly by a NAN service. Figure 54 illustrates the message flow of the ranging session setup procedure initiated by a service.

On receipt of the Range_Request primitive, the NAN Engine constructs and transmits a Ranging Request frame to start the ranging session setup procedure.

On receipt of the Ranging Request frame, the NAN Engine checks whether “Auto Response” is set to true. If “Auto Response” is set to false, a Range_Request_Inidication event is generated and sent to the application layer. The application layer either rejects or commences the event transaction by initiating the Range_Response primitive.

On receipt of the Range_Response primitive or if the “Auto Response” is set to true, the NAN Engine constructs and transmits the Ranging Response frame to the peer entity.

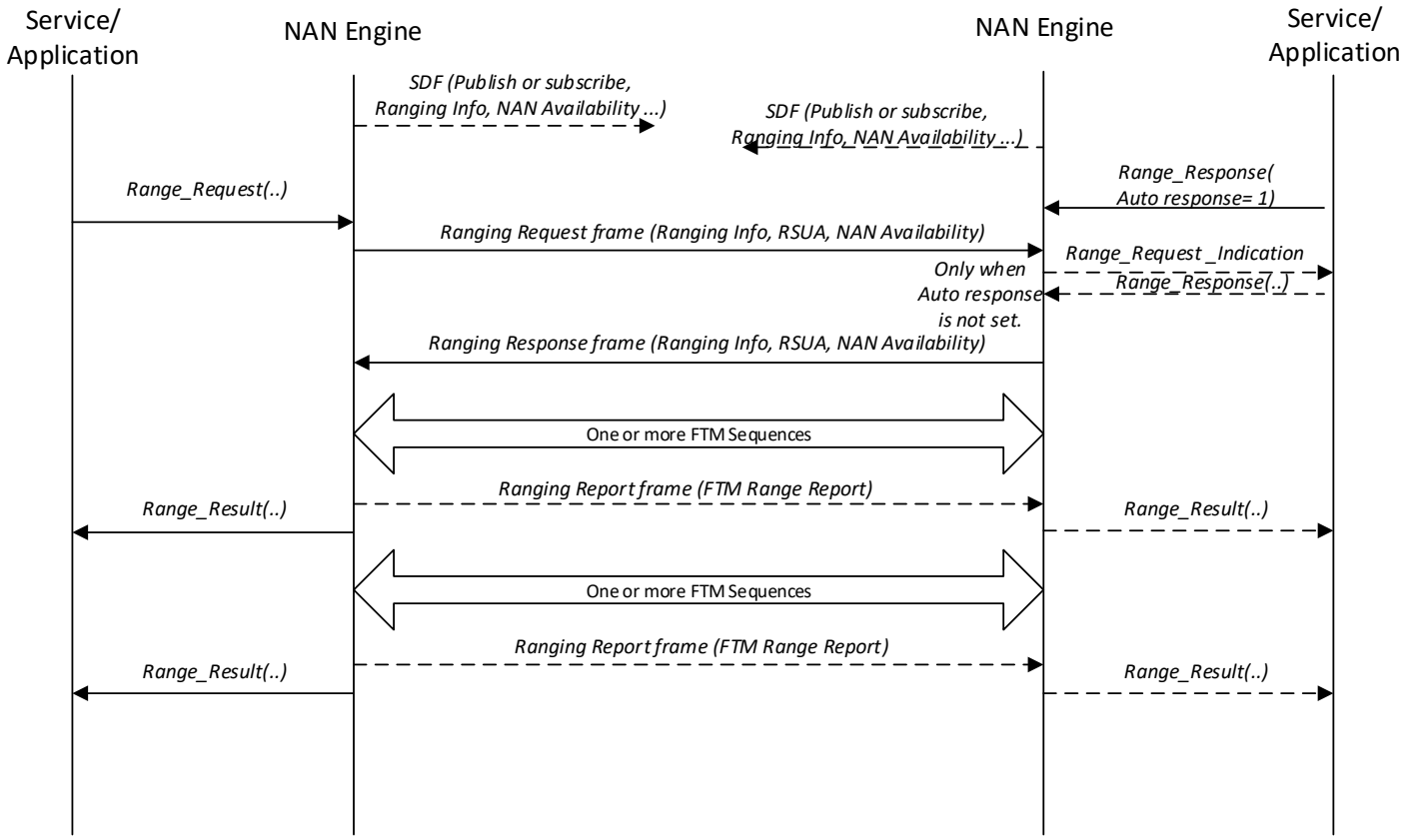


Figure 54. Ranging session invoked by a NAN service

8.3.3 NAN ranging invoked as a part of service discovery

The NAN Ranging session setup may be initiated as a part of service discovery. Figure 55 illustrates the message flow of the ranging session setup procedure initiated by a Publish service.

Upon receipt of the SDF (a Publish service discovery) with the Ranging Required bit set to true in the Service Descriptor Extension attribute, the NAN Engine constructs and transmits a Ranging Request frame to the peer NAN Device that transmitted this unsolicited Publish SDF frame to start the ranging session setup procedure for the intended service.

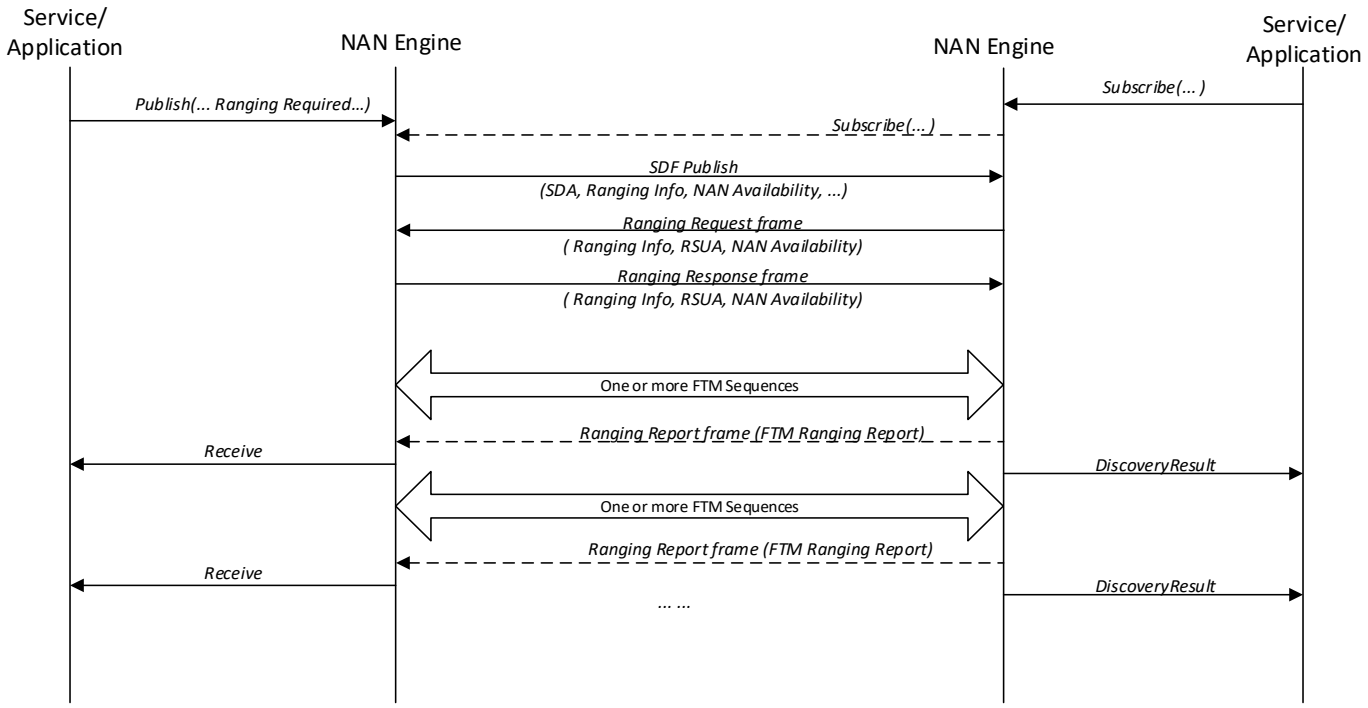


Figure 55. Ranging session invoked by a Publish service

8.3.4 NAN ranging session setup

The NAN Device that starts the ranging session setup is the Ranging Initiator. The responding device is the Ranging Responder. The Ranging Initiator and Ranging Responder act as the FTM Initiator (i.e., Initiating STA) and FTM Responder (i.e. Responding STA) of the corresponding FTM session, respectively.

During the NAN Ranging session setup, two NAN Ranging devices establish the ranging schedule by exchanging their Potential, Conditional, and Committed FAWs. The ranging schedule, once established, consists of one or more ranging CRBs, which are essentially the overlapped portions of the two NAN Ranging Devices' Committed FAWs selected by the time bitmap in the Ranging Setup attribute. The two NAN Ranging devices should ensure the ranging schedule includes sufficient ranging CRBs to support the required FTM parameters.

The Ranging Initiator starts the ranging session setup procedure by transmitting a Ranging Request frame to the Ranging Responder. The Ranging Request frame shall include the Ranging Information attribute, Ranging Setup attribute and NAN Availability attribute.

The NAN FTM Parameters field of the Ranging Setup attribute in the Ranging Request frame provides proposed NAN FTM parameters for the ranging operation.

The Map ID field, Time Bitmap Control field, Time Bitmap Length field, and the Time Bitmap field in the Ranging Setup attribute provide a proposed ranging schedule and point to the NAN Availability attribute associated with the Potential, Conditional, or Committed FAWs.

On receipt of the Ranging Request frame or the Range_Response primitive, the NAN Engine constructs and transmits a Ranging Response frame to the peer entity.

The Ranging Response frame shall include the Ranging Setup attribute and may include the NAN Availability attribute.

The Status subfield of the Ranging Setup attribute in the Ranging Response frame shall be set to either zero (Accepted) or one (Rejected). If the Status subfield is set to one (Rejected), a reason code shall be specified in the Reason Code field. The NAN Availability attribute should be included in the Ranging Response frame if the rejection is for a scheduling reason i.e. the Reason Code is set to RANGING_SCHEDULE_UNACCEPTABLE. If the Status subfield is set to zero (Accepted), the Reason Code field is reserved, and the NAN Availability attribute shall be included in the Ranging Response frame. The FTM parameters, Map ID, and Time bit map information is optional in the Ranging Response frame when the value of the Status subfield in the Ranging Setup attribute is set to "Rejected". The presence or absence of the

NAN FTM Parameters field and Ranging Schedule Entry List field shall be indicated using the corresponding bits in the Ranging Control field of the Ranging Setup attribute.

The Ranging Report Required bit of the Ranging Setup attribute in the Ranging Response frame set to one indicates that the ranging report is required by the Ranging Responder. Otherwise, Ranging Report Required should be set to zero. This field is reserved in the frame transmitted by the Ranging Initiator.

The NAN FTM Parameters field in the Ranging Setup attribute that is included in the Ranging Response frame provides a final set of the NAN FTM parameters for the ranging operation. The responding NAN Device's selection of the NAN FTM parameters should meet the requirements of the proposed NAN FTM Parameters from the Ranging Request frame. If the responding NAN device cannot meet the requirements, the device should reject the ranging request by setting the value of the Status subfield in the Ranging Setup attribute to "Rejected", and the value of the Reason Code field to FTM_PARAMETERS_INCAPABLE.

The Map ID field, Time Bitmap Control field, Time Bitmap Length field, and Time Bitmap field of the Ranging Setup attribute in the Range Response frame provide a ranging schedule and point to the NAN Availability attribute to indicate the Committed FAW that the NAN device will be present.

If the responding NAN Device cannot be present on any FAWs that are included in Ranging Request frame, the device should reject the ranging request by setting the value of the Status subfield in the Ranging Setup attribute to "Rejected", and the value of the Reason Code field to RESOURCE_LIMITATION.

The responding Ranging device may reject the ranging request for any other reasons, as described in Table 43. For example, the responding Ranging device may reject the ranging request due to "No Movement" based on the last movement indication in the Ranging Info attribute of the Ranging Request frame.

8.3.5 NAN ranging session update

A Ranging Initiator may initiate a ranging session update by transmitting a Ranging Request frame to the Ranging Responder.

A Ranging Responder may request a ranging session update by transmitting a Schedule Update Notification NAF including Potential, Conditional, or Committed FAWs. Upon receipt of the Schedule Update Notification NAF, the Ranging Initiator may decide to initiate a ranging session update.

The ranging session update procedure is same as the ranging session setup procedure, as defined in section 8.3.4.

8.3.6 NAN ranging session termination

On the receipt of the Cancel_Range primitive, a NAN Ranging device shall terminate the ranging session by transmitting the Ranging Termination frame to the peer ranging device.

A NAN Ranging Device may decide to terminate a ranging session for any reason at any time by transmitting the Ranging Termination frame to the peer ranging device. Either the Ranging Initiator or the Ranging Responder may terminate the ranging session.

If the ranging session is terminated, the committed resource blocks located for the corresponding ranging session shall be released.

8.3.7 FTM Range Report to the Ranging Responder

When the Ranging Report Required bit in the Ranging Setup attribute of the Ranging Response frame is set to one, the Ranging Initiator shall transmit a Ranging Report frame including the FTM Range Report attribute to the Ranging Responder upon completion of each FTM session (i.e., each single block). Examples of the FTM Range Report sent to the Responder are illustrated in Figure 54 and Figure 55.

8.3.8 FTM protocol and procedure

The FTM protocol, as defined in [1] and illustrated in Figure 56, shall operate with ASAP=1 and single burst mode.

The Single Burst ASAP FTM (single burst, ASAP=1) procedure shall operate each CRB of the established ranging schedule, which consists of one of more ranging CRBs. If the NAN Ranging session is a periodic ranging session, the repeat interval of the Single Burst ASAP FTM session is indicated in the Period subfield of the Time Bitmap Control field of the Ranging Response frame.

During each scheduled ranging CRB, the Ranging Initiator shall send an Initial FTM Request frame to the responding device to start a Single Burst ASAP FTM session. Note that the FTM parameters Min Delta FTM and FTM Format and Bandwidth that are included in the Initial FTM Request frame shall be the same as the parameters that were included in the latest Ranging Response frame. The Ranging Initiator may change other parameters in the Initial FTM Request frame, however the changed parameters are only valid for the current burst instance.

A Single Burst ASAP FTM session should be completed within the CRB allocated for the single burst indicated by the Time Bitmap field in the Ranging Setup attribute of the Ranging Response frame. The Ranging Initiator and Ranging Responder may cease ranging operation (i.e. stop transmitting or receiving FTM messages) outside the CRB indicated in the Ranging Session Setup procedure. NAN ranging relies on NAN synchronization and hence the optional TSF Synchronization sub-feature of FTM (refer to [1] section 9.6.8.33) should not be used with NAN ranging.

The Ranging Initiator should transmit the Initial FTM Request frame at the beginning of the scheduled ranging resource block. If the required number of FTM measurement frames in the burst are completed, the Ranging Initiator or Ranging Responder may cease ranging operation in the scheduled ranging CRB. Note that a ranging operation in the scheduled ranging CRB may be ceased, but the NAN Ranging session shall not be terminated unless a Ranging Termination frame is transmitted. The Ranging session termination is described in section 8.3.6.

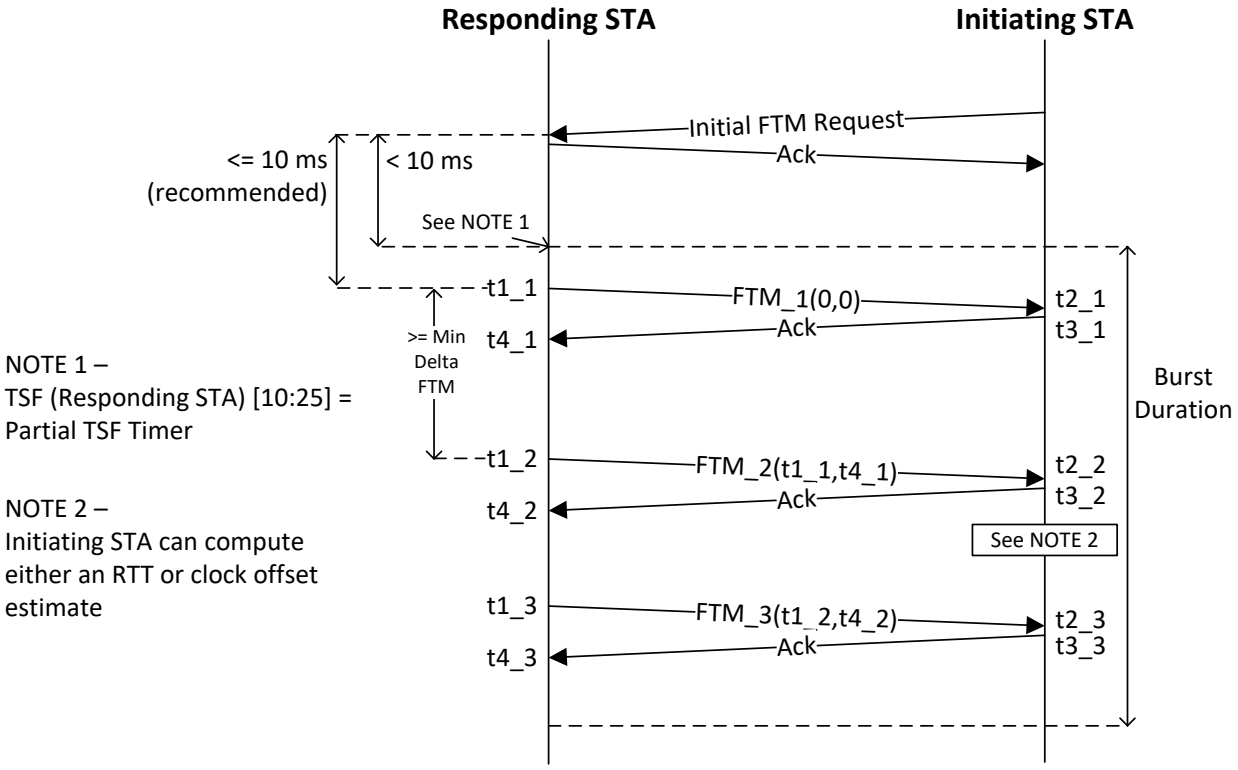


Figure 56. FTM Protocol with Single Burst and ASAP Mode

9 NAN Information Element, attributes, and frame formats

This section defines the frame formats, information elements, and attributes for NAN Devices and the NAN communication protocol.

The NAN communication protocol uses the following:

1. NAN attributes are incorporated in NAN Information Elements (NAN IE) that are carried in NAN Synchronization and NAN Discovery Beacon frames, as well as the PASN Authentication frames. The NAN IE is a Vendor Specific Information Element with the Wi-Fi Alliance OUI and a Wi-Fi Alliance OUI type to indicate NAN operation.
2. NAN attributes in NAN Service Discovery frames (SDF). A NAN SDF is a Public Action frame or Protected Dual of Public Action frame (unicast only) and utilizes the Vendor Specific Public Action frame formats defined in [1] with the Wi-Fi Alliance OUI and Wi-Fi Alliance OUI type indicating NAN operation.
3. NAN attributes in a NAN Action frame (NAF). A NAN NAF is a Public Action frame or Protected Dual of Public Action frame (unicast only) and utilizes the Vendor Specific Public Action frame formats defined in [1] with the Wi-Fi Alliance OUI and Wi-Fi Alliance OUI type indicating NAN Management Operations.

Multiple NAN attributes are defined by this specification in section 9.5. The NAN IE may carry one or more NAN attributes.

A NAN Device is required to properly generate and decode, and if needed, fragment and defragment the NAN IEs and support transmission and reception of the NAN protocol frames for NAN protocol operation.

9.1 NAN Information Element format

The Vendor Specific information element format (as defined in [1]) shall be used to define the NAN IE in this specification. The format of the NAN IE is shown in Table 29.

Table 29. NAN IE format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific information element
Length	1	Variable	Length of the following fields in the IE in octets. The Length field is variable, and set to 4 plus the total length of the NAN attributes.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI
OUI Type	1	0x13	Identifying the type and version of the NAN IE
NAN attributes	Variable	Variable	One or more NAN attribute

NOTE: The NAN IE is subject to element fragmentation and defragmentation, as defined section 10.28.11 and 10.28.12 of [1], if its payload size is larger than 255 octets.

9.2 NAN Synchronization and NAN Discovery Beacon frame format

This section defines the format for the NAN Synchronization and NAN Discovery Beacon frames. These NAN Beacon frames are based on a modified IEEE 802.11 Beacon Management frame. NAN Beacon frames may be protected with an 802.11 Management MIC as defined in the section 12.5.4.2 (BIP MMPDU format) of [1] when an BIGTKSA exists for the NMI address used for the Beacon. When protected, the MIC shall be carried in an 802.11 Management MIC element (MME) that appears immediately before the frame FCS field.

The NAN Synchronization Beacon frame shall have a maximum MMPDU of 128 octets and the NAN Discovery Beacon frame shall have a maximum MMPDU of 350 octets. The NAN Beacon frames shall carry the NAN IE that in turn can carry one or more NAN attribute as long as the maximum size is not exceeded. The NAN Synchronization and NAN Discovery Beacon frame format is shown in Figure 57.

1

Octets:	2	2	6	6	6	2	8	2	2	Var.	8 or 16	4
	FC	**Duration**	**A1**	**A2**	**A3**	**Seq. Ctrl**	**Time Stamp**	**Beacon Interval**	**Capability**	**NAN IE**	**MME**	**FCS**

Figure 57. NAN Synchronization and NAN Discovery Beacon frame format

Where:

- FC is the Frame Control field as defined in [1]. The fromDS and toDS bits within the Frame Control field shall be set to zero
- Duration is the duration value for the beacon frame as defined in [1]
- A1 is set to the broadcast address
- A2 is the transmitter MAC address
- A3 is the Cluster ID that identifies the NAN Cluster and is described in section 9.5.2
- Seq. Ctrl. is the sequence control field as defined in [1]
- Time Stamp is the time stamp for the beacon frame as defined in [1]
- Beacon Interval field is as defined in [1]. The Beacon Interval field shall be set to 512 TUs in NAN Synchronization Beacon frames, which corresponds to the time between consecutive starts of Discovery Windows. For NAN Discovery Beacon frames, the Beacon Interval field shall be set to 100 TUs, which corresponds to the average time between consecutive NAN Discovery Beacon transmissions transmitted by the same NAN Device in Master role. However, as described in section 3.3.8.1 the exact transmission time of NAN Discovery Beacon frames may deviate from the target beacon transmission time (TBTT)
- Capability is the capability information field as defined in [1]. The capability bits for: Spectrum Mgmt., QoS, APSD, Radio Measurement, Delayed Block ACK and Intermediate Block ACK may be set as defined in [1]. The remaining capabilities bits shall be set as shown in Table 30

Table 30. NAN Synchronization Beacon Capability Information field

b0	b1	b2	b3	b4	b5	b6	b7
0	0	0	0	0	1	0	0

b8	b9	b10	b11	b12	b13	b14	b15
Spectrum Mgmt	**QoS**	1	**APSD**	**Radio Measurement**	0	**Delayed Block Ack**	**Immediate Block Ack**

The NAN IE is defined in section 9.1 and has a variable length depending on the number of NAN attributes found in the NAN IE field.

The MME is optionally present in NAN Beacon frames, and if present, appears last in the frame body to protect the frame, as specified in section 12.5.4 (Broadcast/multicast integrity protocol (BIP)) of [19].

FCS is the frame checksum for the beacon frame as defined in [1].

Table 31 defines the NAN attributes allowed or not allowed to be included in NAN Beacon frames; and, if allowed, whether they are mandatorily (M) or optionally (O) included. The mandatory NAN attributes shall be inserted in the NAN Beacon frames in the order specified in Table 31.

Table 31. NAN attributes in NAN Beacon frames

Attributes	**NAN Beacon frames**	
	Synchronization	**Discovery**
Master Indication attribute	YES/M	YES/M
Cluster attribute	YES/M	YES/M
Service ID List attribute	YES/O	YES/O

Attributes	NAN Beacon frames	
	Synchronization	**Discovery**
Subscribe Service ID List attribute	YES/O	YES/O
Service Descriptor Attribute	NO	NO
NAN Connection Capability attribute	NO	NO
WLAN Infrastructure attribute	NO	NO
P2P Operation attribute	NO	NO
IBSS attribute	NO	NO
Mesh attribute	NO	NO
Further NAN Service Discovery attribute	NO	NO
Further Availability Map attribute	NO	NO
Country Code attribute	YES/O	YES/O
Ranging attribute	NO	NO
Cluster Discovery attribute	NO	NO
Service Descriptor Extension attribute	NO	NO
Device Capability attribute	YES/O	YES/O
Device Capability Extension attribute	YES/O	YES/O
Transmit Power Envelope attribute	YES/O	YES/O
NDP attribute	NO	NO
NAN Availability	YES/O	YES/O
NDC attribute	YES/O	YES/O
NDL attribute	NO	NO
NDL QoS Attribute	NO	NO
Unaligned Schedule attribute	YES/O	YES/O
S3 attribute	NO	NO
Ranging Information attribute	YES/O	YES/O
Ranging Setup attribute	NO	NO
FTM Ranging Report attribute	NO	NO
Element Container attribute	YES/O	YES/O
Extended WLAN Infrastructure attribute	YES/O	YES/O
Extended P2P Operation attribute	YES/O	YES/O
Extended IBSS attribute	YES/O	YES/O
Extended Mesh attribute	YES/O	YES/O
Cipher Suite Info attribute	NO	NO
Security Context Info attribute	NO	NO
Shared-Key Descriptor attribute	NO	NO
Public Availability attribute	YES/O	YES/O

Attributes	NAN Beacon frames	
	Synchronization	Discovery
Vendor Specific attribute	YES/O	YES/O

9.3 NAN Service Discovery frame format

The NAN Service Discovery frame (SDF) is a Vendor Specific Public Action frame as defined in [1]. The format and the values for the NAN SDF are defined in Table 32.

Table 32. NAN Service Discovery frame format

Field	Size (Octets)	Value (Hex)	Description
Category	1	0x04 or 0x09	IEEE 802.11 Public Action frame or Protected Dual of Public Action frame (see section 9.6.10 of [1])
Action	1	0x09	IEEE 802.11 Public Action frame Vendor Specific
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI
OUI Type	1	0x13	Identifying the type and version of the NAN
NAN attributes	Variable	Variable	One or more NAN attributes
MME	8 or 16	Variable	The MME is optionally present in group addressed SDFs, and if present, appears last in the frame body to protect the frame, as specified in section 12.5.4 (Broadcast/multicast integrity protocol (BIP)) of [19].

Table 33 defines the NAN attributes allowed or not allowed to be included in NAN SDF frames; and, if allowed, whether they are mandatorily (M) or optionally (O) included. The mandatory NAN attributes shall be inserted in the NAN SDF frames in the order specified in Table 33.

Table 33. NAN attributes in NAN SDF frames

Attributes	NAN SDF frames				
	Publish			Subscribe	Follow-up
	Data Required	Ranging Required	Otherwise		
Master Indication attribute	NO	NO	NO	NO	NO
Cluster attribute	NO	NO	NO	NO	NO
Service ID List attribute	NO	NO	NO	NO	NO
Service Descriptor attribute	YES/M	YES/M	YES/M	YES/M	YES/M
NAN Connection Capability attribute	YES/O	YES/O	YES/O	YES/O	YES/O
WLAN Infrastructure attribute	YES/O	YES/O	YES/O	YES/O	YES/O
P2P Operation attribute	YES/O	YES/O	YES/O	YES/O	YES/O
IBSS attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Mesh attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Further NAN Service Discovery attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Further Availability Map attribute	YES/O	YES/O	YES/O	YES/O	YES/O

Attributes	NAN SDF frames				
	Publish			Subscribe	Follow-up
	Data Required	Ranging Required	Otherwise		
Country Code attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Ranging attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Cluster Discovery attribute	NO	NO	NO	NO	NO
Service Descriptor Extension attribute	YES/M	YES/M	YES/O	YES/O	YES/O
Device Capability attribute	YES/M	YES/M	YES/O	YES/O	YES/O
Device Capability Extension attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Transmit Power Envelope attribute	YES/O	YES/O	YES/O	YES/O	YES/O
NDP attribute	NO	NO	NO	NO	NO
NAN availability	YES/M	YES/M	YES/O	YES/O	YES/O
NDC attribute	YES/O	YES/O	YES/O	YES/O	YES/O
NDL Attribute	NO	NO	NO	NO	NO
NDL QoS attribute	NO	NO	NO	NO	NO
Unaligned Schedule attribute	YES/O	YES/O	YES/O	YES/O	YES/O
S3 attribute	NO	NO	NO	NO	NO
Ranging Information attribute	NO	YES/M	NO	NO	YES/O
Ranging Setup attribute	NO	NO	NO	NO	NO
FTM Ranging Report attribute	NO	NO	NO	NO	NO
Element Container attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Extended WLAN Infrastructure attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Extended P2P Operation attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Extended IBSS attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Extended Mesh attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Cipher Suite Info attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Security Context Info attribute	YES/O	YES/O	YES/O	YES/O	YES/O
Shared-Key Descriptor attribute	NO	NO	NO	NO	NO
Public Availability attribute	YES/O	YES/O	YES/O	YES/O	YES/O
NAN Identity Resolution attribute	YES/O	YES/O	YES/O	YES/O	YES/O
NAN Pairing Bootstrapping attribute	YES/O	YES/O	YES/O	YES/O	YES/O

Attributes	NAN SDF frames				
	Publish			Subscribe	Follow-up
	Data Required	Ranging Required	Otherwise		
Vendor Specific attribute	YES/O	YES/O	YES/O	YES/O	YES/O

9.4 NAN Action frame format

9.4.1 General format

The NAN Action frame (NAF) is a Public Action frame (as defined in [1]). The general format of the NAN Action frame is shown in Table 34. Table 35 contains NAN Action frame subtypes.

Table 34. General format of NAN Action frame format

Field	Size (Octets)	Value (Hex)	Description
Category	1	0x04 or 0x09	IEEE 802.11 Public Action frame or IEEE 802.11 Protected Dual of Public Action frame.
Action	1	0x09	IEEE 802.11 Public Action frame Vendor Specific
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI
OUI Type	1	0x18	Identifying the type and version of the NAN
OUI Subtype	1	Variable	Identifying the type of NAN Action frame. The specific value is defined in Table 35
Information Content	Variable	Variable	Including fields and/or attributes for each specific NAN action frames, as defined in the following sections.
MME	8 or 16	Variable	The MME is optionally present in group addressed NAFs, and if present, appears last in the frame body to protect the frame, as specified in section 12.5.4 (Broadcast/multicast integrity protocol (BIP)) of [19].

Table 35. NAN Action frame subtypes

OUI Subtype	Notes
0	Reserved
1	Ranging Request
2	Ranging Response
3	Ranging Termination
4	Ranging Report
5	Data Path Request
6	Data Path Response
7	Data Path Confirm
8	Data Path Key Installment
9	Data Path Termination
10	Schedule Request
11	Schedule Response
12	Schedule Confirm
13	Schedule Update Notification

OUI Subtype	Notes
14 – 255	Reserved

9.4.2 Ranging frames

The Ranging frames use the NAN Action frame format. These are the Ranging Request frame, Ranging Response frame, Ranging Termination frame, and Ranging Report frame.

The Ranging Request frame and Ranging Response frame are transmitted by NAN Ranging devices to setup or update the ranging session. The Ranging Termination frame is transmitted by the NAN Ranging device to terminate the ranging session. The Ranging Report frame is transmitted by a NAN Ranging device to send ranging measurements to another NAN Ranging device. The attributes included in the Ranging Request frame, Ranging Response frame, Ranging Termination frame and Ranging Report frame are defined in Table 36.

Table 36. Attributes included in the Information Content for the Ranging frames

Attributes	Ranging Request	Ranging Response	Ranging Termination	Ranging Report
Ranging FTM Range Report	N	N	N	M
Ranging Info	M	M	O	O
Ranging Setup	M	M	M	N
NAN Availability	M	M (Accepted) O (Rejected)	O	O
Unaligned Schedule	O	O	O	O
Device Capability	M	M (Accepted) O (Rejected)	N	N

9.4.3 Data Path Setup frames

The Data Path Setup frames use the NAN Action frame format. They include the Data Path Request frame, Data Path Response frame, Data Path Confirm frame and Data Path Key Installment frame.

The Data Path Request frame, Data Path Response frame, Data Path Confirm frame and Data Path Key Installment frame are transmitted by NAN Data devices to setup a NAN Data Path. The attributes included in the Data Path Request frame, Data Path Response frame, Data Path Confirm frame and Data Path Key Installment frame are defined in Table 37, Table 38 and Table 39.

Table 37. Attributes included in the Information Content for Data Path setup frames for NDP/NDL setup together without security

Attributes	Data Path Request	Data Path Response			Data Path Confirm (NDP Confirm Required)	Data Path Confirm (NDL Counter)	
		NDL Status			NDP Status	NDL Status	
		A	R	C	A	A	R
NDP or NDPE	M	M	M	M	M	N	N
Device Capability	M	M	O	M	O	O	O
Device Capability Extension	O	O	O	O	O	O	O
Transmit Power Envelope attribute	O	O	O	O	O	O	O
NAN Availability	M	M	O	M	O	M	O
NDC	O	M	O	M	N	M	O

Attributes	Data Path Request	Data Path Response			Data Path Confirm (NDP Confirm Required)	Data Path Confirm (NDL Counter)	
		NDL Status			NDP Status	NDL Status	
		A	R	C	A	A	R
NDL	M	M	M	M	N	M	M
NDL QoS	O	O	O	O	N	O	O
Element Container	M	M	O	M	O	O	O
Unaligned Schedule	O	O	O	O	O	O	O
S3	O	O	O	O	O	O	O

Table 38. Attributes included in the Information Content for Data Path Setup frames for NDP setup only without security

Attributes	Data Path Request	Data Path Response		Data Path Confirm (NDP Confirm Required)
		NDP Status		NDP Status
		A	R	A
NDP or NDPE	M	M	M	M
Device Capability	M	M	O	O
Device Capability Extension	O	O	O	O
Transmit Power Envelope attribute	O	O	O	O
NAN Availability	O	O	O	O
NDC	O	O	O	N
Element Container	M	M	O	O
Unaligned Schedule	O	O	O	O
S3	O	O	O	O

Table 39. Security Attributes included in the Information Content for Data Path Setup with security (in addition to other required attributes)

Attributes	Data Path Request	Data Path Response		Data Path Confirm		Security Key Install	
		NDP Status		NDP Status		NDP Status	
		R	C	R	C	A	R
NDP or NDPE	M	M	M	M	M	M	M
Cipher Suite Information	M	O	M	N	N	N	N
Security Context Information	M	O	M	N	N	N	N
NAN Shared Key Descriptor (NA unless NCS-SK)	M	O	M	O	M	M	O

‘Accepted’ is not acceptable as a NDP status in a Data Path Response and Confirm messages when security is being used. Similarly, ‘Continued’ is not an acceptable NDP status in the Security Key Install message. In addition, the rules for including other attributes in the Data Path Setup frames for NDL/NDP setup together without security also apply when

security is included. The rules for attributes in the Data Path Setup for NDP setup only without NDL setup are also the same.

A ND_PMKID received in a Data Path response is optional and indicates the responder is using the ND-PMK that was identified in the Data Path request. The Initiator may or may not support receiving a different ND-PMKID than what was identified in the request.

To minimize denial of service, NAN Shared Key descriptor is included in the frames, it should be validated before accepting any status information it may contain.

9.4.4 Schedule frames

Schedule frames use the NAN Action frame format. They include the Schedule Request frame, Schedule Response frame, Schedule Confirm frame and Schedule Update Notification frame.

The Schedule Request frame, Schedule Response frame and Schedule Confirm frame are transmitted by NAN devices to setup a schedule for NAN operations. The Schedule Update Notification frame is transmitted by a NAN Device to announce a schedule update for NAN operations. The attributes included in the Information Content for the Schedule Request, Schedule Response, Schedule Confirm and Schedule Update Notification frames are specified in Table 40.

Table 40. Attributes included in the Information Content for Schedule frames

Attributes	Schedule Request	Schedule Response			Schedule Confirm		Schedule Update Notification
		NDL Status			NDL Status		
		A	R	C	A	R	
Device Capability	O	O	O	O	O	O	O
Device Capability Extension	O	O	O	O	O	O	O
Transmit Power Envelope attribute	O	O	O	O	O	O	O
NAN Availability	M	M	O	M	M	O	M
NDC	O	M	O	M	M	O	O
NDL	M	M	M	M	M	M	N
NDL QoS	O	O	O	O	O	O	O
Element Container	O	O	O	O	O	O	O
Unaligned Schedule	O	O	O	O	O	O	O
S3	O	O	O	O	O	O	O

9.5 NAN attributes

The NAN attributes are defined to have a common general format consisting of a one (1) octet NAN attribute ID field, a 2 octet Length field, and variable-length attribute-specific Information fields, as shown in Table 41.

Table 41. List of NAN attributes

Field	Size (Octets)	Value (Hex)	Description
Attribute ID	1	Variable	Identifies the type of NAN attribute as defined in Table 42
Length	2	Variable	Length of the following fields in the attribute
Attribute Body	Variable	Variable	NAN attribute specific information fields

Table 42 lists all the NAN attributes. Their inclusions in NAN Management frames are specified in sections 0, 9.3, and 9.4.

Table 42. NAN attributes in NAN Beacon frames and NAN SDF

Attribute ID	Description
0x00	Master Indication attribute
0x01	Cluster attribute
0x02	Service ID List attribute
0x03	Service Descriptor attribute
0x04	NAN Connection Capability attribute
0x05	WLAN Infrastructure attribute
0x06	P2P Operation attribute
0x07	IBSS attribute
0x08	Mesh attribute
0x09	Further NAN Service Discovery attribute
0x0A	Further Availability Map attribute
0x0B	Country Code attribute
0x0C	Ranging attribute
0x0D	Cluster Discovery attribute1
0x0E	Service Descriptor Extension attribute
0x0F	Device Capability
0x10	NDP attribute
0x11	Reserved (NMSG attribute)
0x12	NAN Availability
0x13	NDC attribute
0x14	NDL attribute
0x15	NDL QoS attribute
0x16	Reserved (Multicast Schedule attribute)
0x17	Unaligned Schedule attribute
0x18	Reserved (Paging attribute - Unicast)
0x19	Reserved (Paging attribute – Multicast)
0x1A	Ranging Information attribute
0x1B	Ranging Setup attribute
0x1C	FTM Ranging Report attribute
0x1D	Element Container attribute
0x1E	Extended WLAN Infrastructure attribute
0x1F	Extended P2P Operation attribute
0x20	Extended IBSS attribute
0x21	Extended Mesh attribute

Attribute ID	Description
0x22	Cipher Suite Info attribute (CSIA)
0x23	Security Context Info attribute (SCIA)
0x24	Shared-Key Descriptor attribute
0x25	Reserved (Multicast Schedule Change attribute)
0x26	Reserved (Multicast Schedule Owner Change attribute)
0x27	Public Availability attribute
0x28	Subscribe Service ID List attribute
0x29	NDP Extension attribute
0x2A	Device Capability Extension attribute (DCEA)
0x2B	NAN Identity Resolution attribute (NIRA)
0x2C	NAN Pairing Bootstrapping attribute (NPBA)
0x2D	S3 attribute
0x2E	Transmit Power Envelope attribute (TPEA)
0x2F-0x4B	Reserved
0x4C	Not used (to avoid conflict with the 802.11 MME element ID)
0x4D-0xDC	Reserved
0xDD	Vendor Specific attribute
0xDE-0xFF	Reserved
Notes: 1. Cluster Discovery Attribute is intended to be carried in any Beacon frame other than a NAN Beacon and Probe Response frames.	

Table 43 defines the Reason Code field.

Table 43. Reason Code field

Values	Name	Description
0	Reserved	Reserved
1	UNSPECIFIED_REASON	Unspecified reason
2	RESOURCE_LIMITATION	Resource limitation
3	INVALID_PARAMETERS	Invalid parameters
4	FTM_PARAMETERS_INCAPABLE	FTM parameters incapable
5	NO_MOVEMENT	No Movement
6	INVALID_AVAILABILITY	Invalid NAN Availability attribute
7	IMMUTABLE_UNACCEPTABLE	Immutable schedule unacceptable
8	SECURITY_POLICY	Rejected due to device/service security policy
9	QoS_UNACCEPTABLE	QoS requirements unacceptable
10	NDP_REJECTED	NDP request rejected by upper layer
11	NDL_UNACCEPTABLE	NDL schedule proposal unacceptable
12	RANGING_SCHEDULE_ UNACCEPTABLE	Ranging schedule proposal unacceptable

Values	Name	Description
13	PAIRING_BOOTSTRAPPING_REJECTED	Pairing bootstrapping request rejected by upper layer
14 to 255	Reserved	Reserved

9.5.1 Master Indication attribute

The Master Indication attribute contains a NAN Device's preference to serve in the role of Master. The format of the Master Preference attribute is shown in Table 44.

The Master Indication attribute shall be included in the NAN Synchronization and NAN Discovery Beacon frames, as described in Table 44. The use of the Master Indication attribute is described in section 3.3.3.

Table 44. Master Indication attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x00	Identifies the type of NAN attribute.
Length	2	2	Length of the following field in the attribute.
Master Preference	1	0 – 255[1]	Information that is used to indicate a NAN Device's preference to serve as the role of Master, with a larger value indicating a higher preference.
Random Factor	1	0 – 255	A random number selected by the sending NAN Device.
Notes: 1. Values 1 and 255 are used for testing purposes only. A NAN Device shall consider 1 and 255 as valid Master Preference values but shall not use these values during normal operation.			

9.5.2 Cluster attribute

The Cluster attribute contains information regarding the NAN Cluster. The format of the Cluster attributes is illustrated in Table 45.

Table 45. Cluster attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x01	Identifies the type of NAN attribute.
Length	2	13	Length of the following fields in the attribute.
Anchor Master Information	13	Variable	Information about the Cluster's Anchor Master

The Anchor Master Information field format and definition is shown in Table 46.

Table 46. Anchor Master Information field format

Field	Size (Octets)	Value	Description
Anchor Master Rank	8	Variable	Refer to the Master Rank definition in section 3.3.3.
Hop Count to Anchor Master	1	Variable	The number of hops to the Anchor Master.
Anchor Master Beacon Transmission Time	4	Variable	When sent by a Non-Anchor Master Device, carries the lower four (4) octets of the TSF of the transmission time of the Beacon sent by the Anchor Master. When sent by the Anchor Master Device, set to 0x00000000.

9.5.3 Service ID List attribute

The Service ID List attribute contains the NAN Device's service information. The Service IDs used in the NAN Beacon frames are for service announcement/publish purposes. The format of the Service ID List attributes is illustrated in Table 47.

Table 47. Service ID List attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x02	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Service ID	6*N	Variable	One or more Service IDs, where N is the number of Service IDs in this container.

The format of the Service ID field shall be as defined as the Service Hash in[3].

9.5.3.1 Subscribe Service ID List attribute

The Subscribe Service ID List attribute contains the NAN Device's Subscribe service information. The format of the Subscribe Service ID List attributes is illustrated in Table 48.

Table 48. Subscribe Service ID List attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x28	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Service ID	6*N	Variable	One or more Service IDs for Subscribe services, where N is the number of Service IDs in this container.

The format of the Service ID field shall be as defined as the Service Hash in[3].

9.5.4 Service Descriptor

9.5.4.1 Service Descriptor attribute (SDA)

The Service Descriptor attribute is illustrated by Table 49. This attribute contains some mandatory fields and some optional fields depending on the content of the service discovery request, optional filter, and optional service specific information.

Table 49. Service Descriptor attribute format

Field	Size (Octets)	Value (Hex)	Description
Attribute ID	1	0x03	Identifies the type of NAN attribute
Length	2	Variable	Length of the following fields in the attribute.
Service ID	6	Variable	Mandatory field that contains the hash of the Service Name.
Instance ID	1	Variable	Publish_ID or Subscribe_ID Value of zero is reserved
Requestor Instance ID	1	Variable	Instance ID from the frame that triggered the transmission if available, otherwise set to 0x00.
Service Control	1	Variable	Mandatory field that defines the Service Control bitmap as defined in Table 50
Binding Bitmap	0 or 2	0x0000 to0xFF FF	Optional field that indicates the binding of the SDA to post discovery connection attributes

Field	Size (Octets)	Value (Hex)	Description
Matching Filter Length	0 or 1	Variable	An optional field and present if a matching service discovery filter is used
Matching Filter	Variable	Variable	An optional field that is a sequence of length and value pairs that identify the matching service discovery filters, refer to Figure 58
Service Response Filter Length	0 or 1	Variable	An optional field and present if a service response filter is used.
Service Response Filter	Variable	Variable	An optional field that identifies the matching service response filters, refer to Table 52
Service Info Length	0 or 1	Variable	An optional field and present if service specific information is used
Service Info	Variable	Variable	An optional field that contains the service specific information. Its content may be determined by the application and not specified herein.

If a NAN frame includes two or more SDAs, any two SDAs shall not use the same Instance ID.

A NAN Device that supports an optional field of the Service Descriptor may include such an optional field in the NAN Service Discovery frame that it transmits.

The Service Control field is mandatory and is illustrated in Table 50. The Service Control field indicates if the Service Descriptor attribute corresponds to Publish, Subscribe, or Follow-up function and if other optional fields are present in the Service Descriptor attribute such as Matching Filter, Service Response Filter, and Service specific information.

Table 50. Service Control field format

Bit(s)	Information	Notes
0-1	Publish, Subscribe, Follow-up	Identifies the Service Control Type: 00: Publish 01: Subscribe 10: Follow up 11: Reserved
2	Matching Filter Present	If set to 1, a Matching Filter field is found in the Service Descriptor attribute, otherwise set to 0.
3	Service Response Filter Present	If set to 1, a Service Response Filter field is found in the Service Descriptor attribute, otherwise set to 0.
4	Service Info Present	If set to 1, a Service Info field is found in the Service Descriptor attribute, otherwise set to 0.
5	Discovery Range Limited	If set to 1, indicates the Publish/Subscribe message is limited in range to close proximity. If set to 0, indicates the Publish/Subscribe message is not limited in range. Valid only when the message is either of a Publish or a Subscribe type.
6	Binding Bitmap	If set to 1, this bit indicates that a binding bit map is present
7	Reserved	

The requirements for the different fields of the service discovery attributes for transmit and receive operations are defined in Table 51.

Table 51. Transmit and receive side requirements for the Service Descriptor attribute fields

Field	Transmit		Receive
	Capability	Activation	
Service ID	Mandatory	Mandatory	Mandatory
Service Control	Mandatory	Mandatory	Mandatory

Field	Transmit		Receive
	Capability	Activation	
Matching Filter	Optional	Optional	Mandatory
Service Response Filter	Optional	Optional	Mandatory
Service Info	Optional	Optional	Mandatory
Binding Bitmap	Optional	Optional	Mandatory

The Matching Filter Length is an optional field and present if a service discovery filter is used. The Matching Filter field format is illustrated in Figure 58. This field is a sequence of length and value pairs identifying the service discovery filters.

Octets:	1	Variable	1	Variable	1	Variable
	Length	**Filter Value**	**Length**	**Filter Value**	**Length**	**Filter Value**

Figure 58. Matching Filter field format

The Service Response Filter Length is an optional field and present if a service response filter is used. The Service Response Filter enables a potential respondent to determine whether it should respond to the NAN Service Discovery frame. The Service Response Filter is considered only when the respondent has determined that a response may be sent based on the Service ID and Matching Filter. The Service Response Filter field format is defined in Table 52.

Table 52. Service Response Filter field format

Field	Size (Octets)	Value (Hex)	Description
SRF Control	1	Variable	Mandatory field that defines the Service Response Filter Control field bitmap as defined in Table 53
Address Set	Variable	Variable	List MAC Addresses or Bloom Filter as defined section 4.1.9.2.

The Service Response Filter Control field is defined in Table 53.

Table 53. Service Response Filter Control field format

Bit(s)	Information	Notes
0	SRF Type	The SRF Type indicates whether the Address Set is a sequence of MAC addresses or a Bloom Filter. If the SRF Type bit in SRF control is set to 0, then the Address Set is represented as a sequence of MAC Addresses to be carried in the SRF Element. If the SRF Type bit in SRF control is set to 1, then the Address Set is a Bloom filter delivered in the SRF Element. Method of creating the Address Set and determining membership in the Address Set is presented in section 4.1.9.2.
1	Include	Include bit = 0 indicates that STAs present in the Address Set shall not send responses to the received query discovery frame. Include bit =1 indicates that only STAs present in the Address Set shall send a response to a received query discovery frame. Procedures for determining membership in the Address Set are given in in section 4.1.9.2.
2-3	Bloom Filter Index	Identifies the Bloom Filter index being used.
4-8	Reserved	Reserved

The WLAN Infrastructure attribute, P2P Operation attribute, IBSS attribute, Mesh attribute, and Ranging attribute are referred to as post-discovery attributes.

If the Binding Bitmap field is present in an SDA, it indicates that the post discovery operation of the service in the SDA is restricted to operation based on the post discovery attributes in the SDF whose bit positions in the bitmap are set to one (1). Each bit position *i* corresponds to the i^{th} post discovery attribute in the SDF in the order it is present, i.e., the first post discovery attribute from the beginning of the SDF is indicated in the first bit of the bitmap, the second one is indicated by the 2nd bit and so on. If a bit in the bitmap is set to zero, then the operation of the service in the SDA is not permitted through the operation of the corresponding post discovery attribute.

If the Binding Bitmap field is not present in an SDA, the receiving NAN Devices should assume that there is no information available regarding the association of the corresponding service with any post discovery attribute. It is up to the receiving NAN Devices' implementations to decide whether and how to make use of the further availability information included in the received SDF.

NOTE: If a Further NAN Service Discovery attribute is included in a SDF, it indicates the NAN Device is available beyond DWs for discovery of all services that are specified by SDAs included in the same SDF.

9.5.4.2 Service Descriptor Extension attribute

Table 54 defines the Service Descriptor Extension attribute (SDEA).

Table 54. Service Descriptor Extension attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x0E	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Instance ID	1	Variable	The same value as in the Instance ID field of the associated Service Descriptor attribute.
Control	2	Variable	Information about the fields present. See Table 55.
Range Limit	0 or 4	Variable	Range limit given in centimeters. Refer to Figure 59. This is an optional field.
Service Update Indicator	0 or 1	Variable	Monotonically increasing value indicating the current version of the service specific information corresponding to the publish instance, which may be conveyed by publish messages and/or FSD messages. This is an optional field.
Service Info Length	0 or 2	Variable	Length of the Service Info field. An optional field and present if Service Info field is present.
Service Info	Variable	Variable	An optional field that contains the service specific information. The format of Service Info field is shown in Table 57.

Table 55. SDEA Control field format

b0	b1	b2	b3	b4	b5	b6	b7
FSD Required	**FSD with GAS**	**Data Path Required**	**Data Path Type**	**Reserved (Multicast Type)**	**QoS Required**	**Security Required**	**Ranging Required**

b8	b9	b10	b11	b12	b13	b14	b15
Range Limit Present	**Service Update Indicator Present**	**GTK Required**	**Reserved**	**Reserved**	**Reserved**	**Reserved**	**Reserved**

Octets:	2	2
	Bytes 0-1	Bytes 2-3
	Ingress Range Limit	**Egress Range Limit**

Figure 59. SDEA Range Limit field format

The SDEA is used to carry additional information for service discovery. If implemented, the SDEA should be sent with an SDA in the same frame. The instance ID field carries the instance ID of the associated SDA. The descriptions for the sub-fields of the SDEA control field are given in Table 56.

Table 56. SDEA Control field format

Field	Size (Octets)	Value	Description
FSD Required	b0	Variable	0 otherwise 1 if Further Service Discovery is required for this service
FSD with GAS	b1	Variable	0 if Follow up is used for FSD, Valid only if FSD required is set to 1. Reserved otherwise 1 if GAS is used for FSD
Data Path Required	b2	Variable	0 – no NDP associated with the service 1 – service requires set up of NDP
Data Path Type	b3	Variable	0 – Unicast NDP required 1 – Reserved Reserved if the Data Path Required field is set to 0
Reserved (Multicast Type)	b4	Variable	0 – One to many 1 – Many to Many The field is valid only if Data Path type is set to 1, reserved otherwise
QoS Required	b5	Variable	0 – QoS is NOT required 1 – QoS is required
Security Required	b6	Variable	0 – otherwise 1 – Security required for the NDP associated with the service, Reserved if Data Path Required is set to 0
Ranging Required	b7	Variable	1 – Ranging required prior to subscription for the service, 0 otherwise
Range Limit	b8	Variable	0 otherwise 1 – If Range Limit is specified for the service Valid only if Ranging Required is set to 1, reserved otherwise
Service Update Indicator Present	b9	Variable	0 – otherwise 1 – if the Service Update Indicator field is present.
GTK Required	b10	Variable	0 - otherwise 1 – GTK protection required for group-addressed data frames transmitted and received for the service
Reserved	b10-b15	NA	Reserved

The ingress range and egress range limit for the service are specified in the Range Limit field (refer to Figure 59). The units for the Range limit field are in centimeters.

The Service Info Length is an optional field and present if a Service Info field is present. The format of the Service Info field is shown in Table 57.

Table 57. Service Info field format

Field	Size (Octets)	Value	Description
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI
Service Protocol Type	1	Variable	Indicate service protocol types. The values are shown in Table 58.
Service Specific Info	Variable	Variable	Contain service specific information

If the OUI subfield is set to 0x50-6F-9A (Wi-Fi Alliance specific OUI), the Service Protocol Type subfield is included subsequently. The values of the Service Protocol Type subfield are shown in Table 58.

If the OUI subfield is set to a value other than Wi-Fi Alliance specific OUI, the remaining content of the Service Info field is not specified herein.

The Service Specific Info subfield contains the service specific information. Its content may be determined by the application and not specified herein.

Table 58. Service Protocol Types

Value	Description
0	Reserved
1	Bonjour
2	Generic
3	CSA Matter
4-255	Reserved

The recommended practices for conveying DNS-SD [9] is based on the Generic service protocol .

9.5.5 NAN Connection Capability attribute

The NAN Connection Capability attribute contains a set of parameters that can be used for post NAN Discovery to establish a connection. The format of the NAN Connection Capability attribute is shown in Table 59. Table 60 defines the NAN Connection Capability Bitmap format.

Table 59. NAN Connection Capability attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x04	Identifies the type of NAN attribute.
Length	2	2	Length of the following fields in the attribute.
Connection Capability Bitmap	2	Variable	A set of parameters indicating NAN Device's connection capabilities, as defined in Table 60.

Table 60. NAN Connection Capability Bitmap format

Bit(s)	Information	Notes
0	Wi-Fi Direct	The Wi-Fi Direct field shall be set to 1 if the NAN Device supports Wi-Fi Direct, and is set to 0 otherwise.
1	P2Ps	The P2Ps field shall be set to 1 if the NAN Device supports Wi-Fi Direct Services, and is set to 0 otherwise.
2	TDLS	The TDLS field shall be set to 1 when the NAN Device supports TDLS, and is set to 0 otherwise.
3	WLAN Infrastructure	The WLAN Infrastructure field shall be set to 1 when the NAN Device currently connect to an WLAN Infrastructure AP, and is set to 0 otherwise.
4	IBSS	The IBSS field shall be set to 1 when the NAN Device supports IBSS, and is set to 0 otherwise.
5	Mesh	The Mesh field shall be set to 1 when the NAN Device supports Mesh, and is set to 0 otherwise.
6 – 15	Reserved	—

The use of the NAN Connection Capability attribute is described in section 4.3.

9.5.6 WLAN Infrastructure attribute

The use of this attribute is obsolete.

The WLAN Infrastructure attribute contains a set of parameters that can be used with the Further Availability Map attribute for post NAN Discovery to establish a connection with a WLAN infrastructure network. The format of WLAN Infrastructure attribute is shown in Table 61.

Table 61. WLAN Infrastructure attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x05	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
BSSID	6	Variable	BSSID of the AP.
MAC Address	6	Variable	Device's infrastructure interface address
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 62.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN Device that sets the ith bit of the Availability Intervals Bitmap to 0 may be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute.
Device Role	1	Variable	Identifies the Device role in the WLAN Infrastructure, 0 means AP and 1 means non-AP STA.

The format of the Map Control field is shown in Table 62.

Table 62. Map Control field format for the WLAN Infrastructure attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received; 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

The use of the WLAN Infrastructure attribute is described in section 4.3.

9.5.7 P2P Operation attribute

The use of this attribute is obsolete.

The P2P Operation attribute contains a set of parameters that can be used with the Further Availability Map attribute for post NAN Discovery to establish a P2P connection. The format of the P2P Operation attribute is shown in Table 63.

Table 63. P2P Operation attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x06	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
P2P Device Role	1	Variable	Indicates roles of P2P device, as defined in Table 64.
MAC Address	6	Variable	Device's P2P Device Address.
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 65.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 0 may be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute.

The format of the P2P Device Role bitmap is provided in Table 64.

Table 64. P2P Device Role Bitmap format

Bit(s)	Information	Notes
0	P2P Device	The P2P Device field bit shall be set to 1 if the device operates as P2P Device who can start a new P2P group, and is set to 0 otherwise.
1	P2P Group Owner	The P2P Group Owner field bit shall be set to 1 if the device operates as P2P Group Owner, and is set to 0 otherwise.
2	P2P Client	The P2P Client field bit shall be set to 1 if the device operates as P2P Client, and is set to 0 otherwise.
3 – 7	Reserved	—

The format of the Map Control field is shown in Table 65.

Table 65. Map Control field format for the P2P Operation attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received. 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

The use of the P2P Operation attribute is described in section 4.3.

9.5.8 IBSS attribute

The use of this attribute is obsolete.

The IBSS attribute contains a set of parameters that can be used with the Further Availability Map attribute for post NAN Discovery to establish a connection with a WLAN IBSS network. The format of IBSS attribute is illustrated in Table 66.

Table 66. IBSS attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x07	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
BSSID	6	Variable	BSSID of the IBSS.
MAC Address	6	Variable	Device's IBSS interface address
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 67.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN Device that sets the i^{th} bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN device that sets the i^{th} bit of the Availability Intervals Bitmap to 0 may be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute.

The format of the Map Control field is shown in Table 67.

Table 67. Map Control field format for the IBSS attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received; 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

9.5.9 Mesh attribute

The use of this attribute is obsolete.

The Mesh attribute contains a set of parameters that can be used with the Further Availability Map attribute for post NAN Discovery to establish a connection with a Mesh network. The format of Mesh attribute is illustrated in Table 68.

Table 68. Mesh attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x08	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.

Field	Size (Octets)	Value	Description
MAC Address	6	Variable	Device's Mesh interface address
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 69.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN device that sets the i^{th} bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN device that sets the i^{th} bit of the Availability Intervals Bitmap to 0 may be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute.
Mesh ID	Variable (0..32 octets)	Variable	As defined in section 9.4.2.99 of [1] Mesh ID element

The format of the Map Control field is shown in Table 69.

Table 69. Map Control field format for the Mesh attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received; 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

9.5.10 Further NAN Service Discovery attribute

The Further NAN Service Discovery attribute contains a set of parameters that can be used together with the Further Availability Map attribute to indicate a NAN Device's availability during intervals between DWs to receive NAN Service Discovery frames. The format of Further NAN Service Discovery attribute is illustrated in Table 70.

Table 70. Further NAN Service Discovery attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x09	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 71.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 0 may be present during the corresponding ith time interval in the operation channel indicated by the associated Further Availability Map attribute.

The format of the Map Control field is shown in Table 71.

Table 71. Map Control field format for the Further NAN Service Discovery attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received; 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

9.5.11 Further Availability Map attribute

The Further Availability Map attribute contains a set of parameters that can be used with WLAN Infrastructure attribute, P2P Operation attribute, IBSS attribute, Mesh attribute, or Further NAN Service Discovery attribute to indicate a NAN Device's availability during intervals between DWs for further NAN service discovery or post NAN Discovery operations.

The format of Further Availability Map attribute is illustrated in Table 72.

Table 72. Further Availability Map attribute format

Field	Size (Octets)	Value)	Description
Attribute ID	1	0x0A	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Map ID	1	Variable	Identifies the Further Availability Map attribute. Value 16 – 255 are reserved.
Availability Entry List	Variable	Variable	Including one or more Availability Entries. The format of Availability Entry is defined in Table 73.

The format of Availability Entry List is illustrated in Table 73.

Table 73. Availability Entry List field format for the Further Availability Map attribute

Field	Size (Octets)	Value	Description
Entry Control	1	Variable	Availability Entry control information, as defined in Table 74.
Operating Class	1	Variable	Indicating the frequency band the NAN Device will be available as defined in [19]. Annex E Table E-4 Global Operating Classes.
Channel Number	1	Variable	Indicating the channel the NAN Device will be available.
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Entry Control field. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding ith time interval in the operation channel indicated by the Operating Class and Channel Number fields in the same Availability Entry. A NAN device that sets the ith bit of the Availability Intervals Bitmap to 0 may be present during the corresponding ith time interval in the operation

Field	Size (Octets)	Value	Description
			channel indicated by the Operating Class and Channel Number fields in the same Availability Entry.

The format of the Entry Control field is shown in Table 74.

Table 74. Entry Control field format for the Further Availability Map attribute

Bit(s)	Information	Notes
0-1	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
2-7	Reserved	—

The use of the Further Availability Map attribute is described in section 4.3.

9.5.12 Country Code attribute

The Country Code attribute enables a NAN Device to indicate its current local regulation domain. The format of the Country Code attribute is illustrated in Table 75.

Table 75. Country Code attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x0B	Identifies the type of NAN attribute.
Length	2	2	Length of the following fields in the attribute.
Condensed Country String	2	Variable	The Condensed Country String field is set to the first two octets of the value contained in the dot11CountryString attribute as specified in [1].

9.5.13 Ranging attribute

The Ranging attribute is denoted in Table 76 and provides information for the execution of post discovery ranging. Use of IEEE 802.11 Fine Time Measurement Protocol is indicated by setting the Ranging Protocol value to zero.

The use of the Ranging attribute specified in this section is obsolete. The new attributes to be used are the Ranging Information and Ranging Setup attribute (refer to sections 0 and 9.5.19).

Table 76. Ranging attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x0C	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
MAC Address	6	Variable	Device MAC address for execution of ranging protocol
Map Control	1	Variable	The availability channel and time map control information, as defined in Table 77.
Ranging Protocol	1	Variable	0: Denotes FTM (refer to [1]) 1-255 Reserved
Availability Intervals Bitmap	Variable	Variable	The Availability Intervals Bitmap divides the time between the beginnings of consecutive Discovery Windows of a given NAN cluster into consecutive time intervals of equal durations. The time interval duration is specified by the Availability Interval Duration subfield of the Map Control field. A NAN device that sets the i^{th} bit of the Availability Intervals Bitmap to 1 shall be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute. A NAN

Field	Size (Octets)	Value	Description
			device that sets the i^{th} bit of the Availability Intervals Bitmap to 0 may be present during the corresponding i^{th} time interval in the operation channel indicated by the associated Further Availability Map attribute.

The format of the Map Control field is shown in Table 77.

Table 77. Map Control field format for the Ranging attribute

Bit(s)	Information	Notes
0-3	Map ID	Identifies the associated Further Availability Map attribute
4-5	Availability Interval Duration	Indicates the availability interval duration associated with the Availability Intervals Bitmap field. The value is set as follows: 0: 16 TU; 1: 32 TU; 2: 64 TU; 3: reserved
6	Repeat	0: the signaled availability applies only to the time interval between the beginnings of two consecutive DWs, during which the corresponding attribute is received; 1: the signaled availability repeats for future intervals between DWs for 16 intervals, or until it is changed by a NAN Service Discovery frame that carries different availability information, whichever comes earlier.
7	Reserved	—

9.5.14 Cluster Discovery attribute

The Cluster Discovery attribute is illustrated in Table 78.

Table 78. Cluster Discovery attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x0D	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Cluster ID	6	Variable	NAN Cluster ID
Cluster Time Offset	8	Variable	2's complement representation of the signed difference between the senders TSF and the NAN TSF
Anchor Master Rank	8	Variable	Rank of the Anchor Master of the NAN whose Cluster ID is indicated in the attribute. Refer to the Master Rank definition in section 3.3.3

The Cluster Discovery attribute may be included in a NAN IE carried in a Beacon frame (other than a NAN beacon) or Probe Response frame. Probe Response frames including NAN IE may be sent in response to any probe request if the sender has information of an existing NAN Cluster.

9.5.15 Device Capability attribute

The Device Capability attribute indicates a NAN device's capability. The Device Capability attribute may be included in NAN Management frames for a NAN device to indicate its capabilities. The format of the Device Capability attribute is defined in Table 79.

Table 79. Device Capability attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x0F	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.

Field	Size (Octets)	Value	Description
Map ID	1	Variable	b0: set to 1 to indicate the device capabilities only apply to the specified NAN Availability map. set to 0 to indicate the device capabilities apply to the device, when no NAN Availability map is included in the same frame, or apply to all NAN Availability maps included in the same frame. b1-b4: indicate the NAN Availability map associated with the device capabilities; and reserved when b0 is set to 0. b5-b7: reserved
Committed DW Info	2	Variable	Refer to Table 80
Supported Bands	1	Variable	Bitmap of Band IDs Bit 0: Reserved (for TV white spaces) Bit 1: Sub-1 GHz (excluding TV white spaces) Bit 2: 2.4 GHz Bit 3: Reserved (for 3.6 GHz) Bit 4: 4.9 and 5 GHz Bit 5: Reserved (for 60 GHz) Bit 6: Reserved (for 45 GHz) Bit 7: 6 GHz
Operation Mode	1	Variable	See Table 81
Number of Antennas	1	Variable	Bit 0 -3: Number of TX antennas Value 0 indicates the information is not available. Bit 4-7: Number of RX antennas Value 0 indicates the information is not available.
Max Channel Switch Time	2	Variable	Indicates max channel switch time in units of microseconds. Value 0 indicates the information is not available. Note: Max Channel Switch Time value should be the same across multiple Device Capability attributes included in a single frame.
Capabilities	1	Variable	Bit 0 (DFS Master): Set to 1 indicates that the device is a DFS master device. Otherwise, set to 0. Bit 1 (Extended Key ID): Set to 1 indicates that the device supports IEEE 802.11 extended key ID mechanism (refer to [1] section 9.4.2.24.4 and 12.7.6.4], otherwise, set to 0. If this bit is set to 0, the Key ID 0 shall be used. Bit 2 (Simultaneous NDP data reception): Set to 0 to indicate that the NAN Device does not support to receive the data packets of NDPs belonging to the same NDI pair in more than one channel within any Committed FAW or ULW. The NAN Device's behavior when this bit is set to 1 is outside the scope of this specification. Bit 3 (NDPE attribute support): Set to 1 to indicate that the NAN Device supports the NDPE attribute; set to 0 otherwise. Bit 4 (S3 capable): Set to 1 to indicate that the NAN Device supports S3; set to 0 otherwise. Bit 5 to Bit 7: Reserved.

Table 80. Committed DW Information field format

Field	Size (bits)	Value	Description
2.4 GHz DW	b0-b2	Variable	Value 0 indicates no wake up for any 2.4 GHz DW, which can be used if there is another Device Capability attribute indicating Committed available at DW0. Wake up every 2^(n-1) Value 6 and 7 are reserved Note: for S1G band, it indicates S1G NAN channel DW
5 GHz DW	b3-b5	Variable	Value 0 indicates no wake up for any 5 GHz DW

Field	Size (bits)	Value	Description
			Wake up every 2^(n-1) Value 6 and 7 are reserved
2.4 GHz DW Overwrite	b6-b9	Variable	Map ID of the associated NAN Availability attribute, which the 2.4 GHz DWs take precedence over
5 GHz DW Overwrite	b10-b13	Variable	Map ID of the associated NAN Availability attribute, which the 5 GHz DWs take precedence over
Reserved	b14-b15	Reserved (0)	Reserved

Table 81. Operation Mode field format

Subfield	Size (bits)	Value	Description
PHY Mode	b0, b4	Variable	b0 = 1: VHT b0 = 0: HT only b4 = 1: HE b4 = 0: HE not supported Note: If the device supports both VHT and HE, bits b0 and b4 are set to 1
HE/VHT 80+80	b1	Variable	1: HE/VHT 80+80 support 0: otherwise
HE/VHT 160	b2	Variable	1: HE/VHT 160 support 0: otherwise
Reserved (Paging NDL Support)	b3	Variable	1: P-NDL supported 0 P-NDL not supported
Reserved	b5-b7	Reserved (0)	Reserved

9.5.16 Data Path attributes

9.5.16.1 NAN Data Path attribute

Table 82 defines the NDP attribute.

Table 82. NDP attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x10	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Dialog Token	1	Variable	Set to a nonzero value to identify the request and response transaction.
Type and Status	1	Variable	Bit 0 to Bit 3: Type subfield. The Type subfield identifies the type of the attribute. The values are defined as follows: 0: Request 1: Response 2: Confirm 3: Security Install 4: Terminate 5 to 15: Reserved Bit 4 to Bit 7: Status subfield. The Status subfield identifies the status of the operation associated with the attribute. The values are defined as follows: 0: Continued 1: Accepted 2: Rejected 3 to 15: Reserved

Field	Size (octets)	Value	Description
			The relationship between the Type subfield and the Status subfield is specified in Table 83.
Reason Code	1	Variable	Identifies the reason when the Status subfield is set to “Rejected”. This field is reserved when the Status subfield is set to other values. The values of Reason Code are defined in Table 43.
Initiator NDI	6	Variable	NDP Initiator’s Data Interface Address
NDP ID	1	1 - 255	NDP Identifier (created by the initiator) Value zero is reserved
NDP Control	1	Variable	See Table 84 for details
Publish ID	1	Variable	Optional field. Present only if Type subfield is set to “Request”. Service instance ID for the Publish service.
Responder NDI	6	Variable	Optional field. Present only if Type subfield is set to “Response”, and the Status subfield is set to “Continued” or “Accepted”. NDP Responder’s Data Interface Address
NDP Specific Info	Variable	Variable	Information that is opaquely carried through the NAN

Table 83. Relationship between Type subfield and Status subfield in NDP Attribute

		Type				
		Request	**Response**	**Confirm**	**Security Install**	**Terminate**
Status	Continued	Allowed	Allowed	Allowed	Reserved	Reserved
	Accepted	Reserved	Allowed	Allowed	Allowed	Reserved
	Rejected	Reserved	Allowed	Allowed	Allowed	Reserved

Table 84. NDP Control field

	Confirm Required	**Reserved**	**Security Present**	**Publish ID Present**	**Responder NDI Present**	**NDP Specific Info Present**	**Reserved**
Bit position:	b0	b1	b2	b3	b4	b5	b6-7

The NDP attribute is included in an NAF to negotiate the setup of an NDP between two devices.

Dialog Token identifies the NDP setup sequence. The Type subfield indicates if the attribute corresponds to a request, response, confirm, or security install. The Status subfield indicates the status of the response when the type is response and is reserved otherwise. The Reason Code field specifies the reason for rejection if the status is rejected and is reserved otherwise. The Reason Code field values are specified in Table 43. The Initiator NDI indicates the NDP Initiator’s NDI MAC address.

The NDP ID is a one-octet identifier created by the NDP Initiator to identify the NDP. The combination of the Initiator NDI and the NDP ID uniquely identifies the NDP.

The NDP control field is show in Table 84. The subfields of the NDP Control field are shown in Table 85.

Publish ID Present identifies the Publish service instance associated with the NDP.

Responder NDI Present indicates the NDP Responder’s NDI MAC address.

The NDP Specific Info Present field carries NDP and/or service information that is opaque to NAN.

Table 85. Sub fields of NDP Control field format

Field	Size (bits)	Function
Confirm Required	b0	Valid for joint NDP/NDL setup and when the Type subfield is set to “Request”. Reserved otherwise. 0 – Confirm not required from NDP/NDL Initiator 1 – Confirm required from NDP/NDL Initiator
Reserved	b1	Reserved
Security Present	b2	0 – the NDP does not require security. 1 – the NDP requires security, and the associated security attributes are included in the same NAF.
Publish ID Present	b3	0 – the Publish ID field is not present 1 – the Publish ID field is present
Responder NDI Present	b4	0 – the Responder NDI field is not present 1 – the Responder NDI field is present
NDP Specific Info present	b5	0 – the NDP Specific Info field is not present 1 – the NDP Specific Info field is present
Reserved	b6-b7	Reserved

9.5.16.2 NAN Data Path Extension attribute

Table 86 defines the NDPE attribute.

Table 86. NAN Data Path Extension attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x29	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Dialog Token	1	Variable	Set to a nonzero value to identify the request and response transaction.
Type and Status	1	Variable	Bit 0 to Bit 3: Type subfield. The Type subfield identifies the type of the attribute. The values are defined as follows: 0: Request 1: Response 2: Confirm 3: Security Install 4: Terminate 5 to 15: Reserved Bit 4 to Bit 7: Status subfield. The Status subfield identifies the status of the operation associated with the attribute when the Type subfield is set to Response and is reserved otherwise. The values are defined as follows: 0: Continued 1: Accepted 2: Rejected 3 to 15: Reserved The relationship between the Type subfield and the Status subfield is specified in Table 86.
Reason Code	1	Variable	Identifies the reason when the Status subfield is set to “Rejected”. This field is reserved when the Status subfield is set to other values. The values of Reason Code are defined in Table 43.
Initiator NDI	6	Variable	NDP Initiator’s Data Interface Address
NDP ID	1	1 - 255	NDP Identifier (created by the Initiator) Value zero is reserved
NDPE Control	1	Variable	See Table 87 for details

Field	Size (octets)	Value	Description
Publish ID	1	Variable	Optional field. Present only if Type subfield is set to “Request”. Service instance ID for the Publish service.
Responder NDI	6	Variable	Optional field. Present only if Type subfield is set to “Response”, and the Status subfield is set to “Continued” or “Accepted”. NDP Responder’s Data Interface Address
TLV List	Variable	Variable	A list of TLV fields, as specified in Table 89

The subfields of the NDPE Control field are described in Table 87.

Table 87. Subfields of NDPE Control field format

Field	Size (bits)	Function
Confirm Required	b0	Valid for joint NDP/NDL setup and when the Type subfield is set to “Request”. Reserved otherwise. 0: Confirm not required from NDP/NDL Initiator 1: Confirm required from NDP/NDL Initiator
Reserved	b1	Reserved
Security Present	b2	0: the NDP does not require security. 1: the NDP requires security, and the associated security attributes are included in the same NAF.
Publish ID Present	b3	0: the Publish ID field is not present 1: the Publish ID field is present
Responder NDI Present	b4	0: the Responder NDI field is not present 1: the Responder NDI field is present
GTK Required	b5	0: GTK protection is not required for the NDP 1: GTK protection is required for the NDP
Reserved	b6-b7	Reserved

The NDPE attribute is included in an NAF to negotiate the setup of an NDP between two devices that support the NDPE attribute.

Dialog Token identifies the NDP setup sequence. The Type subfield indicates if the attribute corresponds to a request, response, confirm, or security install. The Status subfield indicates the status of the response when the Type subfield is set to Response and is reserved otherwise. The Reason Code field specifies the reason for rejection if the Status subfield is set to Rejected and is reserved otherwise. The Reason Code field values are specified in Table 43. The Initiator NDI indicates the NDP Initiator’s NDI MAC address.

The NDP ID is a one-octet identifier created by the NDP Initiator to identify the NDP. The combination of the Initiator NDI and the NDP ID uniquely identifies the NDP.

The TLV List contains a list of TLV fields, as specified in Table 88.

Table 88. General TLV format for the NDPE attribute

Field	Size (octets)	Value	Description
Type	1	Variable	Identifies the type of the TLV, as specified in Table 89.
Length	2	Variable	The length in octets of the fields following the length field in the TLV.
Value	Variable	Variable	The value of the TLV.

Table 89. List of TLV Types for the NDPE attribute

Type field value	Description
0x00	IPv6 Link Local, as specified in Table 90
0x01	Service Info, as specified in Table 91
0x02-0xFF	Reserved

Table 90. IPv6 Link Local TLV format

Field	Size (octets)	Value	Description
Type	1	0x00	Identifies the type of the TLV
Length	2	0x08	The length in octets of the fields following the length field in the TLV.
Interface Identifier	8	Variable	The interface identifier is prefixed with a 64-bit network component of fe80:0000:0000:0000 to form a 128-bit IPv6 link local address. For example, if the interface identifier is 1122:3344:5566:7788 then the IPv6 link local address would be fe80:0000:0000:0000:1122:3344:5566:7788.

Table 91. Service Info TLV format

Field	Size (octets)	Value	Description
Type	1	0x01	Identifies the type of the TLV
Length	2	Variable	The length in octets of the fields following the length field in the TLV.
OUI	3	Variable	Vendor OUI
Body	Variable	Variable	Service info body

If the OUI subfield is set to a value other than 0x50-6F-9A (Wi-Fi Alliance specific OUI), the Body field is implementation specific.

If the OUI subfield is set to 0x50-6F-9A (Wi-Fi Alliance specific OUI), the Service Info TLV format is shown in Table 91.

Table 92. Wi-Fi Alliance Service Info TLV format

Field	Size (octets)	Value	Description
Type	1	0x01	Identifies the type of the TLV
Length	2	Variable	The length in octets of the fields following the length field in the TLV.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI
Service Protocol Types	1	Variable	Indicate service protocol types. The values are shown in Table 58.
Service Specific Info	Variable	Variable	Contain service specific information

9.5.17 Schedule attributes

9.5.17.1 NAN Availability attribute

The format of the NAN Availability attribute is shown in Table 93.

Table 93. NAN Availability attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x12	Identifies the type of a NAN attribute.
Length	2	Variable	The length in octets of the fields following the length field in the attribute.
Sequence ID	1	Variable	An integer value that identifies the sequence of the advertised availability schedule. It is incremented by one when any schedule change flag in the Attribute Control field is set to 1; otherwise, it remains unchanged.
Attribute Control	2	Variable	Refer to Table 94.
Availability Entry List	Variable	Variable	Including one or more Availability Entries. The format of an Availability Entry List is defined in Table 95.

The format of the Attribute Control field is given in Table 94.

Table 94. Attribute Control field format for the NAN Availability attribute

Field	Size (bits)	Value	Description
Map ID	4	Variable	Identify the associated NAN Availability attribute
Committed Changed	1	0 or 1	Set to 1 if Committed Availability changed, compared with last schedule advertisement; or any Conditional Availability is included. Set to 0, otherwise. This setting shall be the same for all the maps in a frame
Potential Changed	1	0 or 1	Set to 1 if Potential Availability changed, compared with last schedule advertisement. Set to 0, otherwise. This setting shall be the same for all the maps in a frame
Public Availability Attribute Changed	1	0 or 1	Set to 1 if Public Availability attribute changed, compared with last schedule advertisement. Set to 0, otherwise.
NDC Attribute Changed	1	0 or 1	Set to 1 if NDC attribute changed, compared with last schedule advertisement. Set to 0, otherwise.
Reserved (Multicast Schedule Attribute Changed)	1	0 or 1	Set to 1 if Multicast Schedule attribute changed, compared with last schedule advertisement. Set to 0, otherwise.
Reserved (Multicast Schedule Change Attribute Changed)	1	0 or 1	Set to 1 if Multicast Schedule Change attribute changed, compared with last schedule advertisement. Set to 0, otherwise.
Reserved	6	Reserved (0)	Reserved

Availability Entry

An Availability Entry indicates a NAN Device's Potential, Conditional, or Committed availability within one or more FAWs on one or a set of channels. The format of the Availability Entry is shown in Table 95.

Table 95. Availability Entry field format for the NAN Availability attribute

Field	Size (octets)	Value	Description
Length	2	Variable	The length of the fields following the Length field in the attribute, in the number of octets.
Entry Control	2	Variable	See Table 96 for details.
Time Bitmap Control	2	Variable	Indicates the parameters associated with the subsequent Time Bitmap field. See Table 97 for details.

Field	Size (octets)	Value	Description
Time Bitmap Length	1	Variable	Indicate the length of the following Time Bitmap field, in the number of octets.
Time Bitmap	Variable	Variable	Each bit in the Time Bitmap corresponds to a time duration indicated by the value of Bit Duration subfield in the Time Bitmap Control field. When the bit is set to 1, the NAN Device indicates its availability for any NAN operations for the whole time duration associated with the bit. When the bit is set to 0, the NAN Device indicates unavailable for any NAN related operations for the time duration associated with the bit.
Band/Channel Entry List	Variable	Variable	The list of one or more Band or Channel Entries corresponding to this Availability Entry. See Table 98 for details.

Entry Control field

The format of the Entry Control field is specified in Table 96.

Table 96. Entry Control field format for the NAN Availability attribute

Number of Bit(s)	Information	Notes
0-2	Availability Type	b0: 1, Committed; 0, otherwise; b1: 1, Potential; 0, otherwise. b2: 1, Conditional; 0, otherwise. 000, 101, and 111 are reserved. Note – At least one of the three bits is set to 1 to be meaningful.
3-4	Usage Preference	An integer ranging from 0 to 3, which represents the preference of being available in the associated FAWs. The preference is higher when the value is set larger. Note: It does not apply to Committed or Conditional FAWs.
5-7	Utilization	Values 0 – 5 indicating proportion within the associated FAWs that are already utilized for other purposes quantized to 20%. Value 6 is reserved. Value 7 indicates unknown utilization.
8-11	Rx Nss	Indicate the max number of spatial streams the NAN Device can receive during the associated FAWs.
12	Time Bitmap Present	1: Time Bitmap Control, Time Bitmap Length, and Time Bitmap fields are present 0: Time Bitmap Control, Time Bitmap Length, and Time Bitmap are NOT present, and all NAN Slots are available
13-15	Reserved	Reserved

Time Bitmap Control field

The definition of the Time Bitmap Control field is as shown in Table 97.

Table 97. Time Bitmap Control field format for the NAN Availability attribute

Bit(s)	Field	Notes
0-2	Bit Duration	0:16 TU 1:32 TU 2:64 TU 3:128 TU 4-7 reserved
3-5	Period	Indicate the repeat interval of the following bitmap. When set to 0, the indicated bitmap is not repeated. When set to non-zero, the repeat interval is:

Bit(s)	Field	Notes
		1:128 TU 2: 256 TU 3: 512 TU 4: 1024 TU 5: 2048 TU 6: 4096 TU 7: 8192 TU
6-14	Start Offset	Start Offset is an integer. The time period specified by the Time Bitmap field starts at the 16 * Start Offset TUs after DW0. Note that the NAN Slots not covered by any Time Bitmap are assumed to be NOT available.
15	Reserved	Reserved

The Bit Duration field specifies the time unit used to describe a FAW. If the corresponding bit in the Time Bitmap is set to one, the entire time duration within the corresponding FAW is available. If the corresponding bit in the Time Bitmap is set to zero, the entire time duration within the corresponding FAW is not available. An appropriate Bit Duration value shall be selected in order to use a single Availability Entry to represent a FAW or a sequence of FAWs. For example, to indicate a sequence of FAWs that are n*16 TUs in length, with a separation of time interval that is m*16 TUs in length, the Bit Duration value can be the greatest common denominator of n and m. Alternatively, multiple Availability Entries can be used to describe FAWs with different lengths, by using different Bit Duration values.

Band/Channel Entries List field

Band/Channel Entries List specifies a list of Band or Channel entries as shown in Table 98.

Table 98. Band/Channel Entries List field format for the NAN Availability attribute

Bit(s)	Field	Description
0	Type	Specifies whether the list refers to a set of indicated bands or a set of operating classes and channel entries. 0: The list is a set of indicated bands. 1: the list is a set of Operating Classes and channel entries
1	Non-contiguous Bandwidth	0: Contiguous bandwidth 1: Non-contiguous bandwidth This field is set to 1 if there is at least one Channel Entry indicates non-contiguous bandwidth.
2-3	Reserved	Reserved
4-7	Number of Band or Channel Entries	The number of band entries or channel entries in the list. Value 0 is reserved.
Variable	Band or Channel Entries	If the Type value is 0, including one or more Band Entries, as shown in Figure 60. The value of each Band Entry is specified by the Table 9-95 Band ID field in [19], which is also quoted in Table 99. If the Type value is 1, including one or more Channel Entries as defined in Table 100.

Figure 60. List of Band Entries format

Table 99. List of Band Entries

Band ID	Meaning
0	Reserved (for TV white spaces)
1	Sub-1 GHz (excluding TV white spaces)
2	2.4 GHz
3	Reserved (for 3.6 GHz)
4	4.9 and 5 GHz
5	Reserved (for 60 GHz)
6	Reserved (for 45 GHz)
7	6 GHz
8-255	Reserved

Channel Entry field

A Channel Entry identifies an Operating Class and one of more applicable channels in the Operating Class. Operating classes are defined by Annex E of [1]. The format of the entry is shown in Table 100.

Table 100. Channel Entry format for the NAN Availability attribute

Field	Size (octets)	Value	Description
Operating Class	1	Variable	Global Operating Class as defined in Table E-4 in Annex E of [19].

Channel Bitmap	2	Variable	Channels are as defined in Annex E of [1] for the given Operating Class. One or more channels are defined per Operating Class.
			If Operating Class less than 131 then
			• Bit i of the Channel Bitmap is set to one when the i^{th} Channel, in increasing numerical order, of the possible channels within the Operating Class is selected, and set to zero otherwise
			Else
			• Bits [7:0] => Start channel number (indicated by channel center frequency index column/Channel Set column) within the Operating Class selected
			• Bits [15:8] => Number of channels including start channel number indicated by bits [7:0] and following channels (indicated in channel center frequency index column/Channel set column) within the Operating Class selected

Primary Channel Bitmap	1	Variable	If exactly one bit is set in the Channel Bitmap subfield, then this field indicates the set of selected preferred primary channels. It is reserved otherwise. The detailed setting of Primary Channel Bitmap is shown in Table 101. For 11ah, this field is a Channel Bitmap extension if the channel bandwidth is 1 MHz. **NOTE:** The field is reserved when the Operating Class field indicates a 20 MHz or 40 MHz bandwidth

Auxiliary Channel Bitmap	2	Variable	Present only if the Non-contiguous Bandwidth field is set to one
			For an 80+80 MHz operating channel width, indicates the channel center frequency index of the 80 MHz channel of frequency segment 1 on which the device operates.
			If Operating Class less than 131 then
			• Bit i of the Auxiliary Channel Bitmap is set to one when the i^{th} Channel, in increasing numerical order, of the possible channels within the Operating Class is selected, and set to zero otherwise
			Else
			• Bits [7:0] => Start channel number (indicated by channel center frequency index column/Channel Set column) within the Operating Class selected

Field	Size (octets)	Value	Description
			• Bits [15:8] => Number of channels including start channel number indicated by bits [7:0] and following channels (indicated in channel center frequency index column/Channel set column) within the Operating Class selected When the whole field is set to zero, the field is ignored.

NOTE: All NAN Devices, including 11n-only NAN Devices, need to interpret all Global Operating Classes as defined in Table E-4 in Annex E of [19].

Table 101. Setting for Primary Channel Bitmap

	b0	b1	b2	b3	b4	b5	b6	b7
20 MHz	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0
40 MHz	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0	Set to 0
80 MHz	Set to 1 if the lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the second lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the third lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the fourth lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 0	Set to 0	Set to 0	Set to 0
80 MHz+80 MHz	Set to 1 if the lowest frequency 20 MHz channel of 80 MHz channel of frequency segment 0 is the preferred primary channel and set to 0 otherwise	Set to 1 if the second lowest frequency 20 MHz channel of 80 MHz channel of frequency segment 0 is the preferred primary channel and set to 0 otherwise	Set to 1 if the third lowest frequency 20MHz channel of 80 MHz channel of frequency segment 0 is the preferred primary channel and set to 0 otherwise	Set to 1 if the fourth lowest frequency 20 MHz channel of 80 MHz channel of frequency segment 0 is the preferred primary channel and set to 0 otherwise	Set to 0	Set to 0	Set to 0	Set to 0
160 MHz	Set to 1 if the lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the second lowest 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the third lowest frequency 20MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the fourth lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the fifth lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the sixth lowest 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the seventh lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise	Set to 1 if the eighth lowest frequency 20 MHz channel is the preferred primary channel and set to 0 otherwise

9.5.17.2 NAN Data Cluster attribute

The NDC attribute contains a set of parameters that describe a NDC. The format of the NDC attribute is given in Table 102.

Table 102. NDC attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x13	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
NDC ID	6	Variable	Identifies the NDC
Attribute Control	1	Variable	Refer to Table 103 for details.
Schedule Entry List	Variable	Variable	One or more schedule entries as defined in Table 104.

Table 103. Attribute Control field format for the NDC attribute

Bit(s)	Information	Notes
b0	Selected NDC	1: Selected NDC for a NDL Schedule. 0: NDC included for the peer's information.
b1-b7	Reserved	Reserved

Table 104. Schedule Entry format for the NDC attribute

Field	Size (octets)	Description
Map ID	1	b0 – b3: Indicates the NAN Availability attribute associated with the subsequent schedule time bitmap. b4 – b7: reserved
Time Bitmap Control	2	Indicates the parameters associated with the subsequent Time Bitmap field. Refer to Table 97 for details.
Time Bitmap Length	1	Indicate the length of the following Time Bitmap field, in the number of octets.
Time Bitmap	Variable	Indicates the time windows associated with the schedule

9.5.17.3 NAN Device Link attribute

The format for the NDL attribute is defined in Table 105.

Table 105. NDL attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x14	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Dialog Token	1	Variable	Set to a nonzero value to identify the request and response transaction.
Type and Status	1	Variable	Bit 0 to Bit 3: Type subfield. The Type subfield identifies the type of the attribute. The values are defined as follows: 0: Request 1: Response 2: Confirm 3 to 15: Reserved Bit 4 to Bit 7: Status subfield. The Status subfield identifies the status of the operation associated with the attribute. The values of the Status subfield are defined as follows: 0: Continued 1: Accepted 2: Rejected 3 to 15: Reserved

Field	Size (octets)	Value	Description
			The relationship between the Type subfield and the Status subfield is specified in Table 106.
Reason Code	1	Variable	Identifies the reason when the Status subfield is set to “Rejected”. This field is reserved when the Status subfield is set to other values. The values of Reason Code are defined in Table 43.
NDL Control	1	Variable	Refer to Table 107 for details.
Reserved (NDL Peer ID)	1	Variable	Optional field. An identifier assigned to the peer STA of the NDL (to be used for paging if required)
Max Idle Period	2	Variable	Optional field. Indicate a period of time in units of 1024TU during which the peer NAN device can refrain from transmitting over the NDL without being terminated.
Immutable Schedule Entry List	Variable	Variable	Optional field. One or more Immutable Schedule entries as defined in Table 104.

The NDL attribute shown in Table 106 is used to set up an NDL between a NDL Initiator and a NDL Responder.

Table 106. Relationship between Type subfield and Status subfield in NDL attribute

		Type		
		Request	**Response**	**Confirm**
Status	Continued	Allowed	Allowed	Reserved
	Accepted	Reserved	Allowed	Allowed
	Rejected	Reserved	Allowed	Allowed

The NDL control field is specified in Table 107.

Table 107. NDL Control field format

Field	Size (bits)	Description
NDL Peer ID Present	1	1: Indicates the NDL Peer ID field is included in the NDL attribute; 0: otherwise
Immutable Schedule Present	1	1: Indicates the Immutable Schedule Entry List is included in the NDL attribute; 0: otherwise
NDC Attribute Present	1	1: Indicates the NDC attribute associated with the NDL schedule is included in the same frame that carries the NDL attribute; 0: otherwise
NDL QoS Attribute Present	1	1: Indicates the NDL QoS attribute associated with the NDL schedule is included in the same frame that carries the NDL attribute; 0: otherwise
Max Idle Period Present	1	1: Indicates the Max Idle Period field is included in the NDL attribute; 0: otherwise
NDL Type	1	1: Reserved (Indicates P-NDL request/response or confirm) 0: Indicates S-NDL
NDL Setup Reason	2	00: NDP 01: FSD using GAS 10: reserved 11: reserved

9.5.17.4 NDL QoS attribute

The NDL QoS attribute contains a set of parameters to specify the QoS requirements for the corresponding NDL Schedule. The format of the NDL QoS attribute is given in Table 108.

Table 108. NDL QoS attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x15	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Minimum time slots	1	Variable	Indicate the minimum number of further available NAN Slots needed per DW interval (512 TU). Set to a value of zero if no preference.
Maximum latency	2	Variable	Indicate the maximum allowed NAN Slots between every two non-contiguous NDL CRBs. Set to the value of 65535 if no preference.

9.5.17.5 Unaligned Schedule attribute

The Unaligned Schedule attribute is defined in Table 109.

Table 109. Unaligned Schedule attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x17	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Attribute Control	2	Variable	Refer to Table 110.
Starting Time	4	Variable	The starting time of the first indicated ULW expressed in terms of the lower 4 bytes of the NAN TSF
Duration	4	Variable	The duration for each ULW in units of microseconds
Period	4	Variable	The time between consecutive ULWs in units of microseconds
Count Down	1	Variable	Number of indicated ULWs. The value of 255 indicates the ULWs does not end until next schedule update. The value of 0 indicates that the remaining ULWs are cancelled.
ULW Overwrite	1	Variable	See Table 110
ULW Control	0 or 1	Variable	Optional field, when NOT present, indicating the NAN Device is NOT available on any channel during all ULWs, and all the following fields are not present; when present, see Table 112
Band ID or Channel Entry	Variable	Variable	If present and the Type value is 00, a Band ID as specified by the Table 9-95 Band ID field in [1], which is also quoted in Table 99. If present, and the Type value is 01 or 10, a Channel Entry as defined in Table 100.

Table 110. Attribute Control field format for the Unaligned Schedule attribute

Field	Size (bits)	Value	Description
Schedule ID	4	Variable	Identify the associated Unaligned Schedule
Reserved	4	Reserved (0)	Reserved
Sequence ID	8	Variable	An integer value that identifies the sequence of the Unaligned Schedule. It is incremented by one when the schedule changes to indicate the freshness of the information contained in the corresponding attribute

Table 111. ULW Overwrite field format

Field	Size (bits)	Value	Description
Overwrite All	1	Variable	Set to 1 when the unaligned schedule takes precedence over all NAN Availability attributes; set to 0, otherwise.
Map ID	4	Variable	When Overwrite All flag set to 0, identify the NAN Availability attribute, which the unaligned schedule takes precedence over; reserved otherwise.
Reserved	3	Reserved (0)	Reserved

Table 112. ULW Control field format

Field	Size (bits)	Value	Description
Type	2	Variable	00: Followed by a Band ID field 01: Followed by Channel Entry field without Auxiliary Channel 10: Followed by a Channel Entry field with Auxiliary Channel 11: Reserved
Channel Availability	1	Variable	1: Indicate the NAN Device is available during the ULWs on the channel specified in the followed Channel Entry field; and the Channel Entry field only specifies one channel 0: Indicate the NAN Device cannot be available on the band or channels specified in the followed Band ID field or Channel Entry field
Rx Nss	4	Variable	Indicate the max number of spatial streams the NAN Device can receive during ULWs, if the Channel Availability subfield is set to 1; otherwise, reserved
Reserved	1	Reserved (0)	Reserved

9.5.17.6 S3 attribute

The S3 attribute is used to indicate a refined availability schedule. The format of the S3 attribute is defined in Table 113.

Table 113. S3 attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	2D	Identifies the type of a NAN attribute.
Length	2	Variable	The length in octets of the fields following the length field in the attribute.
S3 Entry List	Variable	Variable	Includes one or more S3 Entries. The format of an S3 Entry is defined in Table 114.

Table 114. S3 Entry field format for the S3 attribute

Field	Size (octets)	Value	Description
Entry Control	1	Variable	The Entry Control field format is defined in Table 115.
Time Bitmap Control	2	Variable	Indicates the parameters associated with the subsequent Time Bitmap field. See Table 116 for details.
Time Bitmap Length	2	Variable	Indicates the length of the following S3 Time Bitmap field, in the number of octets. Value 0 is reserved.
Time Bitmap	Variable	Variable	Each bit in the bitmap corresponds to a sub slot.

Table 115. Entry Control field format for the S3 Entry field of the S3 attribute

Bit(s)	Information	Notes
0	All Maps	b0: set to 1 indicating the S3 entry applies to all Maps; set to 0 indicating the S3 entry applies to a single Map;
1-4	Map ID	b1 – b4: Map ID if b0 is set to 0; reserved otherwise.
5	Immutable	b5 set to 1 indicating the S3 entry is immutable, set to 0 otherwise.
6-7	Reserved	Reserved

Table 116. Time Bitmap Control field format for the S3 Entry field of the S3 attribute

Bit(s)	Field	Notes
0-1	Bit Duration	b0 – b1: value k indicate 2^k TUs per sub slot, where k=0…3 • k = 0: 1 TU • k = 1: 2 TU • k = 2: 4 TU • k = 3: 8 TU
2-5	Repeat Interval Period	Specifies the repeat interval. When set to 0, indicates bitmap is not repeated. When set to non-zero, the repeat interval is: Value m (1 ≤ m ≤ 10) indicates the repeat interval of 16*2^(m-1) TUs (period from 16 TUs to 8192 TUs) m = 1: 16 TU m = 2: 32 TU m = 3: 64 TU m = 4: 128 TU m = 5: 256 TU m = 6: 512 TU m = 7: 1024 TU m = 8: 2048 TU m = 9: 4096 TU m = 10: 8192 TU Value m > 10 is reserved
6-14	Start Offset	Start Offset is an integer. b6 – b14: value n indicates the S3 Time Bitmap start at (16 * n) TUs after DW0 on a slot (16 TU) boundary.
15	Reserved	Reserved

9.5.18 Ranging Information attribute

The Ranging Information attribute is used for a NAN Ranging device to indicate its Ranging Information. The Ranging Information attribute may be included in the Service Discovery frame, Ranging Request frame and Ranging Response frame. The format of the Ranging Information attribute is defined in Table 117.

Table 117. Ranging Information attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1A	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Location Info Availability	1	Variable	Indicates the device's location information Availability. Bit 0 (LCI Local Coordinates): set to 1 indicates that the device has local coordinates available; otherwise, set to 0.

Field	Size (octets)	Value	Description
			Bit 1(Geospatial LCI WGS84): set to 1 indicates that the device has Geo location available; Otherwise, set to 0. Bit 2 (Civic Location): set to 1 indicates that the device has Civic location available; Otherwise, set to zero. Bit 3 (Last Movement Indication): set to 1 indicates the Last Movement Indication field is present. Otherwise, set to zero. Bit 4- Bit 7: reserved.
Last Movement Indication	2	Variable	The value of the cluster TSF[29:14] at the last detected platform movement. This field is present if the Bit 3 of the Location Availability field is set to one (1).

9.5.19 Ranging Setup attribute

The Ranging Setup attribute (RSUA) is used for a NAN Ranging device to setup, update and terminate a ranging session. The Ranging Setup attribute may be included in the Ranging Request frame, Ranging Response frame and Ranging Termination frame. The format of the Ranging Setup attribute is defined in Table 118.

Table 118. Ranging Setup attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1B	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Dialog Token	1	Variable	Set to a nonzero value to identify the request and response transaction.
Type and Status	1	Variable	Bit 0 to Bit 3: Type subfield. The Type subfield identifies the type of the attribute. The values are defined as follows: 0: Request 1: Response 2: Termination 3 to 15: Reserved Bit 4 to Bit 7: Status subfield. The Status subfield identifies status if the Type subfield is set to “Response”. Otherwise, the Status subfield is reserved. The values are defined as follows: 0: Accepted 1: Rejected 2 to 15: Reserved When the Type subfield is set to “Termination”, the Bit 0, Bit 1 and Bit 2 of the Ranging Control filed shall be set to 0, and NAN FTM Parameters and Ranging Schedule Entry List fields shall not be present.
Reason Code	1	Variable	Identifies the reject reason when the Type subfield is to “Response” and the Status subfield is to “Rejected” or the termination reason when the Type subfield is to “Termination”. This field is reserved when the Type subfield is set to “Request”. The values of Reason Code are defined in Table 43.
Ranging Control	1	Variable	Bit 0 (Ranging Report Required): Set to 1 indicates that Ranging Report is required by the Responder. This field is reserved in the frame transmitted by the initiator. Bit 1: Set to 1 if NAN FTM Parameters is Present, 0 other wise Bit 2: Set to 1 if the Ranging Schedule Entry List field is present, set to 0 otherwise. Bit 3 – Bit 7 reserved
NAN FTM Parameters	3	Variable	Carries FTM Parameters. The format of NAN FTM Parameters is defined in Table 119.
Ranging Schedule Entry List	Variable	Variable	One or more Ranging Schedule Entries as defined in Table 104.

Note: the fields illustrated in Table 119 are derived from section 9.4.2.168 in [1].

Table 119. NAN FTM Parameters field format

Number of Bit(s)	Subfield Name	Description
4	Max Burst Duration	Maximum time of a burst
6	Min Delta FTM	Time from the start of a FTM frame to the start of the following FTM frame in a burst
5	Max FTMs per burst	Maximum Number of successfully sent measurement frames sent in a burst
6	FTM Format and Bandwidth	PHY frame type and bandwidth for FTM measurement frame Note that FTM format and bandwidth used for FTM frames may be non-HT
3	Reserved	Reserved

9.5.20 Fine Timing Measurement (FTM) Range Report attribute

The FTM Range Report attribute is used for the Initiator to transmit FTM Range Report to the Responder. The FTM Range Report attribute is included in the Ranging Report frame. The format for the FTM Range Report Attribute is given in Table 120.

Table 120. FTM Range Report attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1C	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
FTM Range Report	variable	Variable	See definition in section 9.4.2.22.18 Fine Timing Measurement Range report in [1]. Note: The BSSID field contains the MAC address of the NAN device whose range is being reported. When the FTM Range Report is used for an Initiator to transmit FTM Range Report to the Responder, the BSSID field is set to the Responder's MAC address. Note: The TSF reported in the report is the NAN TSF

9.5.21 NAN Security attributes

9.5.21.1 Cipher Suite attribute field

The format for the Cipher Suite attribute field is given in Table 121.

Table 121. Cipher Suite attribute field format

Field	Size (octets)	Value	Description
Cipher Suite ID	1	Variable	1 – NCS-SK-128 Cipher Suite 2 – NCS-SK-256 Cipher Suite 3 – NCS-PK-2WDH-128 Cipher Suite 4 – NCS-PK-2WDH-256 Cipher Suite 5 – NCS-GTK-CCMP-128 Cipher Suite 6 – NCS-GTK-GCMP-256 Cipher Suite 7 – NCS-PK-PASN-128 Cipher Suite 8 – NCS-PK-PASN-256 Cipher Suite Other values are reserved.
Publish ID	1	Variable	Identifies the Publish Service Instance

9.5.21.2 Cipher Suite Information attribute

This Cipher Suite Information attribute (CSIA) is used to indicate the set of cipher suites supported by a publisher and advertised in a Publish message. This attribute is used to indicate the selected cipher suite in NDP setup messages. The format for the Cipher Suite attribute is given in Table 122.

Table 122. Cipher Suite Information attribute (CSIA) field format

Field	Size (octets)	Value	Description
Attribute ID	1	0x22	Identifies the type of NAN attribute
Length	2	Variable	Length of the following fields in the attribute.
Capabilities	1	Variable	Bit field containing device security capabilities that apply to all the cipher suites. Bit 0: • 0: 4 ND-TKSA and NM-TKSA (if applicable) replay counters • 1: 16 ND-TKSA and NM-TKSA (if applicable) replay counter Bit 1 and 2: (Bit 2 is high order) • 00: GTKSA, IGTKSA, BIGTKSA are not supported • 01: GTKSA and IGTKSA are supported, and BIGTKSA is not supported • 10: GTKSA, IGTKSA, and BIGTKSA are supported • 11: Reserved Bit 3: Reserved if GTKSA is not supported. Otherwise • 0: 4 GTKSA replay counters • 1: 16 GTKSA replay counters Bit 4: Reserved if IGTKSA and BIGTKSA are not supported. Otherwise • 0: NCS-BIP-128 (BIP-CMAC-128) is selected for transmit • 1: NCS-BIP_256 (BIP-GMAC-256) is selected for transmit All other bits reserved.
Cipher Suite List	Variable	Variable	One or more NAN Cipher Suite attribute fields defined in Table 121.

9.5.21.3 Security Context Identifier field

The format for the Security Context Identifier (SCID) field is given in Table 123.

Table 123. Security Context Identifier (SCID) field format

Field	Size (octets)	Value	Description
Security Context Identifier Type Length	2	Variable	Identifies the length of the Security Context Identifier field
Security Context Identifier Type	1	Variable	The type of Security Context Identifier. 0 – Reserved 1 – ND-PMKID 2 – 255: Reserved
Publish ID	1	Variable	Identifies the Publish Service Instance
Security Context Identifier	Variable	Variable	Identifies the Security Context. For NCS-SK and NCS-PK-2WDH cipher suites, this field contains the 16 octet ND-PMKID identifying the ND-PMK used for setting up the Secure Data Path.

9.5.21.4 Security Context Information attribute

The Security Context Information attribute is used to advertise the set of available Security Context Identifiers and may appear in a publish message. This attribute is used to indicate the selected Security Context in NDP setup messages. The format for the Security Context Information Attribute is given in Table 124.

Table 124. Security Context Information attribute (SCIA) field format

Field	Size (octets)	Value	Description
Attribute ID	1	0x23	Identifies the type of NAN attribute

Field	Size (octets)	Value	Description
Length	2	Variable	Length of the following fields in the attribute.
Security Context Identifier List	Variable	Variable	Contains one or more Security Context Identifiers defined in Table 123.

9.5.21.5 NAN Shared Key Descriptor attribute

The NAN Shared Key Descriptor attribute contains the 802.11 Key Descriptor as defined in Figure 12-32 EAPOL Key frame of [1]. It does not include the EAPOL header. The format for the NAN Shared Key Descriptor attribute is given in Table 125.

This attribute is included in all NAN Data Path Setup messages when an NCS-SK or NCS-PK-2WDH cipher suite is used for securing the Data Path. For NCS-SK or NCS-PK-2WDH, the key descriptor is used to secure

- The setup of one or more NAN Data Paths
- The exchange itself

Table 125. NAN Shared Key Descriptor attribute field format

Field	Size (octets)	Value	Description
Attribute ID	1	0x24	Identifies the type of NAN attribute
Length	2	Variable	Length of the following fields in the attribute.
Publish ID	1	Variable	Identifies the Publish Service Instance
IEEE 802.11 RSNA Key Descriptor	Variable	Variable	See [1] Figure 12-32 EAPOL Key frame. It begins with the ‘Descriptor Type’ field.

NAN KDE

NAN KDEs are the key descriptor elements carried in the Key Data field of the Key Descriptor in the NAN Shared Key Descriptor attribute. The KDE format is as shown in Figure 12-34 KDE Format of [1]. The OUIs and Data Types used in the NAN KDEs are shown in Table 126.

Table 126. NAN KDE field format

OUI	Data type	Description	Key data encrypted
00-0F-AC	1 (0x01)	GTK KDE	Yes
00-0F-AC	3 (0x03)	MAC address KDE	Yes
00-0F-AC	9 (0x09)	IGTK KDE	Yes
00-0F-AC	14 (0x0E)	BIGTK KDE	Yes
50-6F-9A	36 (0x24)	NIK KDE	Yes
50-6F-9A	37 (0x25)	NAN Key Lifetime KDE	Yes

The formats of the GTK KDE, MAC address KDE, IGTK KDE, and BIGTK KDE are the same as those defined in Figure 12-36, Figure 12-42, and Figure 12-47 of [19].

Note: Other KDEs defined in section 12.7.2 of [19] can also be used as NAN KDEs.

The NIK KDE format is shown in Figure 61. The value of the Cipher Version and the length of the NIK field are specified in Table 22.

Octets:	1	variable
	Cipher Version	NIK

Figure 61. NIK KDE format

The format of the NAN Key Lifetime KDE is shown in Figure 62. The Key Lifetime value is expressed in seconds and uses big endian octet order, same as that defined in Figure 12-40 of [19].

.

Octets:	2	4
	Key Bitmap	Key Lifetime (in seconds)

Figure 62. NAN Key Lifetime KDE format

The format of the Key Bitmap field is shown in Table 63. A bit in the Key Bitmap field is set to one if the Key Lifetime value applies to the corresponding key; otherwise, the bit is set to zero.

Note: More than one bit in the Key Bitmap field can be set to one.

Bits:	b0	b1	b2	b3	b4	b5	b6-b15
	GTK	IGTK	BIGTK	NIK	ND-TK	NM-TK	Reserved

Figure 63. Key Bitmap format

9.5.21.6 NAN Identity Resolution attribute

The NAN Identity Resolution attribute (NIRA) is used by a NAN Device to reveal its long-term identity to a peer device which possesses its NIK.

The format of the NIRA is defined in Table 127.

Table 127. NIRA format

Field	Size (octets)	Value	Description
Attribute ID	1	0x2B	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Cipher Version	1	Variable	0: 128-bit NIK, 64-bit Nonce, 64-bit Tag, HMAC-SHA-256 1-255: reserved
Nonce	Variable	Variable	A random bit string
Tag	Variable	Variable	A resolvable identity

9.5.21.7 NAN Pairing Bootstrapping attribute

The NAN Pairing Bootstrapping attribute (NPBA) is used to enable the pairing bootstrapping between a bootstrapping initiator and a bootstrapping responder.

The format of the NPBA is defined in Table 128.

Table 128. NPBA format

Field	Size (octets)	Value	Description
Attribute ID	1	0x2C	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Dialog Token	1	Variable	Set to a nonzero value to identify the request and response transaction. Reserved when Type = 0 (Advertise)

Field	Size (octets)	Value	Description
Type and Status	1		Bit 0 to Bit 3: Type subfield. The Type subfield identifies the type of the attribute. The values are defined as follows: 0: Advertise 1: Request 2: Response 3 to 15: Reserved Bit 4 to Bit 7: Status subfield 0: Accepted (only applicable to Type = 2, reserved for other Type values) 1: Rejected (only applicable to Type = 2, reserved for other Type values) 2: Comeback (applicable to Type = 1 or Type = 2, reserved for other Type values) 3 to 15: Reserved The Status subfield is reserved for other Type values.
Reason Code	1	Variable	Indicate the reject reason when Type = 2 (Response) and Status = 1 (Rejected); otherwise, reserved
Comeback	Variable	Variable	The format is defined in Table 129. The field is present if: • the Type subfield is set to 2 and the Status subfield is set to 2, or • the Type subfield is set to 1 and the Status subfield is set to 2, and a cookie is required. otherwise, not present
Pairing Bootstrapping Method	2	Variable	b0: set to 1 to indicate opportunistic bootstrapping; set to 0 otherwise b1: set to 1 to indicate pin-code display; set to 0 otherwise b2: set to 1 to indicate passphrase display; set to 0 otherwise b3: set to 1 to indicate QR-code display; set to 0 otherwise b4: set to 1 to indicate NFC tag, set to 0 otherwise b5: set to 1 to indicate keypad (pin-code only); set to 0 otherwise b6: set to 1 to indicate keypad (passphrase); set to 0 otherwise b7: set to 1 to indicate QR-code scan; set to 0 otherwise b8: set to 1 to indicate NFC reader, set to 0 otherwise b9-b13: reserved b14: set to 1 to indicate service managed bootstrapping; set to 0 otherwise b15: set to 1 to indicate bootstrapping handshakes skipped; set to 0 otherwise The field is reserved when Type = 2, and the Status is non-zero.

Table 129. Comeback field format

Field	Size (octets)	Value	Description
Comeback After	0 or 2	Variable	Present if the Type subfield is set to 2 and the Status subfield is set to 2 otherwise, not present Comeback time in TUs after which the receiver is requested to retry the request
Cookie Length	1	Variable	Length of the following cookie
Cookie	Variable	Variable	An opaque sequence of octets generated by the transmitter in an implementation dependent manner

9.5.22 Element Container attribute

The Element Container attribute contains one of more information elements defined in [1]. The format of the Element Container attribute is shown in Table 130.

Table 130. Element Container attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1D	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Map ID	1	Variable	b0: set to 1 to indicate the element only applies to the specified NAN Availability map. set to 0 to indicate the element applies to the device, when no NAN Availability map is included in the same frame, or applies to all NAN Availability maps included in the same frame. b1-b4: indicates the NAN Availability map associated with the element; and reserved when b0 is set to 0. b5-b7: reserved
Elements	Variable	Variable	Contains one or more information elements defined in [1] and [19]

9.5.23 Non-NAN operations

9.5.23.1 Non-NAN Operating Channel Information field

The field shown in Table 131 is used in Non-NAN Operation attributes to describe operating channel information.

Table 131. Non-NAN Operating Channel Information field format

Field	Size (octets)	Value	Description
Global operating class	1	Variable	See [19] Annex E, Table E-4 for detail
Channel	1	Variable	Primary 20MHz channel. Note that primary channel uniquely determines the frequency range for 80MHz, 160MHz and the first segment of 80 + 80 MHz channels.
Channel Center Frequency	1	Variable	For 80 + 80 MHz channels only, indicates the channel center frequency index of the second segment. Set to 0 otherwise.

9.5.23.2 Non-NAN Beacon Information element

The field shown in Table 132 is used in Non-NAN Operation attributes to describe Beacon timing information.

Table 132. Non-NAN Beacon Information field format

Field	Size (octets)	Value	Description
TBTT Offset	2	Variable	The difference in TUs between last NAN DW0 where the 26 LSB bits of NAN TSF were 0 and the NAN TSF of any Non-NAN Beacon that was transmitted after the referred DW0. Set to 0 if the Beacon information is not available.
Beacon Interval	2	Variable	The number of TUs between TBTTs. Set to 0 if the Beacon information is not available.

9.5.23.3 Extended WLAN Infrastructure attribute

The Extended WLAN Infrastructure attribute contains a set of parameters that may be used with the NAN Availability attribute or the Unaligned Schedule attribute to indicate a NAN Device's operation in a WLAN infrastructure network. The format of the Extended WLAN Infrastructure attribute is shown in Table 133.

Table 133. Extended WLAN Infrastructure attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1E	Identifies the type of NAN attribute.

Field	Size (octets)	Value	Description
Length	2	Variable	Length of the following fields in the attribute.
BSSID	6	Variable	BSSID of the AP.
MAC Address	6	Variable	Device's infrastructure interface address
Device Role	1	Variable	Identifies the Device role in the WLAN Infrastructure: 0 means AP; 1 means non-AP STA associated with the AP; 2 means non-AP STA and it is listening to the AP, but not associated with the AP.
Non-NAN Operating Channel Information field	3	Variable	The field is described in Table 131.
Non-NAN Beacon Information	4	Variable	The field is described in Table 132.

9.5.23.4 Extended P2P Operation attribute

The Extended P2P Operation attribute contains a set of parameters that can be used with the NAN Availability attribute or the Unaligned Schedule attribute to indicate a NAN Device's operation in a Wi-Fi P2P network. The format of the Extended P2P Operation attribute is shown in Table 134.

Table 134. Extended P2P Operation attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x1F	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
P2P Device Role	1	Variable	Indicates roles of P2P device, as defined in Table 135
MAC Address	6	Variable	Device's P2P Device Address.
Non-NAN Operating Channel Information	3	Variable	The field is described in Table 131.
Non-NAN Beacon Information	4	Variable	The field is described in Table 132.

The format of the P2P Device Role bitmap is provided in Table 135.

Table 135. P2P Device Role bitmap format

Bit(s)	Information	Notes
0	P2P Device	The P2P Device field bit shall be set to 1 if the device operates as P2P Device who can start a new P2P group, and is set to 0 otherwise.
1	P2P Group Owner	The P2P Group Owner field bit shall be set to 1 if the device operates as P2P Group Owner, and is set to 0 otherwise.
2	P2P Client	The P2P Client field bit shall be set to 1 if the device operates as P2P Client, and is set to 0 otherwise.
3 – 7	Reserved	—

9.5.23.5 Extended IBSS attribute

The Extended IBSS attribute contains a set of parameters that can be used with the NAN Availability attribute or the Unaligned Schedule attribute to indicate a NAN Device's operations in a WLAN IBSS network. The format of the Extended IBSS attribute is illustrated in Table 136.

Table 136. Extended IBSS attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x20	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
BSSID	6	Variable	BSSID of the IBSS.
MAC Address	6	Variable	Device's IBSS interface address
Non-NAN Operating Channel Information	3	Variable	The field is described in Table 131.
Non-NAN Beacon Information	4	Variable	The field is described in Table 132.

9.5.23.6 Extended Mesh attribute

The Extended Mesh attribute contains a set of parameters that can be used with the NAN Availability attribute or the Unaligned Schedule attribute to indicate a NAN Device's operations in a WLAN Mesh network. The format of the Extended Mesh attribute is illustrated in Table 137.

Table 137. Mesh attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x21	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
MAC Address	6	Variable	Device's Mesh interface address
Non-NAN Operating Channel Information	3	Variable	The field is described in Table 131.
Non-NAN Beacon Information	4	Variable	The field is described in Table 132.
Mesh ID	Variable (0..32 octets)	Variable	As defined in section 9.4.2.99 of [1] Mesh ID element

9.5.24 Public Availability attribute

The Public Availability attribute contains a set of parameters that indicate a NAN Device's Committed Availability schedules for all other NAN Devices in the neighborhood. The format of the Public Availability attribute is illustrated in Table 138.

Table 138. Public Availability attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0x27	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Public Availability Schedule Entry List	Variable	Variable	One or more Public Availability Schedule Entries as defined in Table 104.

9.5.25 Vendor Specific attribute

The Vendor Specific Attribute is reserved for vendor specific attributes. The format for the vendor specific attribute is defined in Table 139.

Table 139. Vendor Specific attribute format

Field	Size (octets)	Value	Description
Attribute ID	1	0xDD	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
OUI	3	Variable	Vendor Specific OUI
Body	Variable	Variable	Vendor Specific body that is implementation specific.

9.5.26 Device Capability Extension attribute

The Device Capability Extension (DCEA) attribute indicates a NAN Device's additional capability information.

The format of the Device Capability Extension attribute is defined in Table 140.

Note: Device Capability Extension attribute may be extended by appending new fields.

Table 140. Device Capability Extension attribute format

Field	Size (Octets)	Value	Description
Attribute ID	1	0x2A	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
Capability Info	Variable	Variable	Referring to Table 141

Table 141. Capability Info field

Bits	Value	Description
b0	0 or 1	Set to 1 if Regulatory Info encoding for operation in 6GHz band included in bits b1-b3 Otherwise set to 0
b1-b3	0	Indoor AP An AP whose operation does not require control from an external system such as an Automated Frequency Coordination (AFC) system but that is subject to additional regulatory requirements intended to prohibit outdoor operation.
	1	Standard power AP An AP whose operation requires control from an external system such as an AFC system.
	2	Very low power AP An AP whose operation does not require control from an external system such as an AFC system, is not subject to additional regulatory requirements intended to prohibit outdoor operation and is restricted to very low transmit power.
	3	Indoor enabled AP An AP whose operation relies on being able to successfully receive an enabling signal (as defined by the regulatory rules) from an indoor AP or an indoor standard power AP.
	4	Indoor standard power AP An AP whose operation requires control from an external system such as an AFC system and that is subject to additional regulatory requirements intended to prohibit outdoor operation.
b4-b7		Reserved for Regulatory Info
b8	0 or 1	Set to 1 if pairing setup is enabled, otherwise set to 0
b9	0 or 1	Set to 1 if NPK/NIK caching is enabled, otherwise set to 0 The value of this field is valid only if b8 is set to 1, reserved otherwise
b10-n		Reserved

9.5.27 Transmit Power Envelope attribute

The Transmit Power Envelope attribute (TPEA) conveys a NAN Device's local or regulatory maximum transmit powers based on its NAN availability schedules. The format of the TPEA is illustrated in Table 142.

Table 142. Transmit Power Envelope attribute (TPEA) format

Field	Size (octets)	Value	Description
Attribute ID	1	0x2E	Identifies the type of NAN attribute.
Length	2	Variable	Length of the following fields in the attribute.
TPE Entry List	Variable	Variable	One or more TPE Entries as defined in Table 143.

Table 143. TPE Entry field format for TPEA

Field	Size (octets)	Value	Description
TPE Payload	Variable	Variable	The payload of the Transmit Power Envelope element defined in section 9.4.2.161 of [19], including the Length, Transmit Power Information, and Maximum Transmit Power fields.
Schedule Entry	Variable	Variable	Indicate the NAN availability map and time where the TPE applies to. The Schedule Entry format is defined in Table 104.

9.6 NAN sub-attributes

9.6.1 Generic Service Protocol

This section defines the format for the Service Specific Info field of the SDEA used during NAN service discovery and the NDPE attribute used during data path bring up when the OUI field is set to 0x50-6F-9A (Wi-Fi Alliance specific OUI) and the Service Protocol Types field is set to 2 (Generic).

The Service Specific Info field consists of a sequence of sub-attributes. The format of sub-attributes is shown in Table 144 - Table 153.

Table 144. Generic Service Protocol sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	Variable	Identifies the sub-attribute, as specified in Table 145
Length	2	Variable	The length in octets of the fields following the length field in the sub-attribute
Value	Variable	Variable	Value of the sub-attribute

Table 145. List of sub-attribute IDs for Generic Service Protocol

Sub-attribute ID field value	Description
0x00	Transport Port
0x01	Transport Protocol
0x02	Service Name
0x03	Name of the Service Instance
0x04	TextInfo
0x05	UUID

Sub-attribute ID field value	Description
0x06	BLOB
0x07 – 0xDC	Reserved
0xDD	Vendor Specific Info
0xDE-0xFF	Reserved

Table 146. Transport Port Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x00	Identifies the sub-attribute
Length	2	0x02	The length in octets of the fields following the length field in the sub-attribute
Port Number	2	Variable	Port number used by the transport layer protocol

Table 147. Transport Protocol Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x01	Identifies the sub-attribute
Length	2	0x01	The length in octets of the fields following the length field in the sub-attribute
Transport Protocol	1	Variable	Transport Protocol Number assigned by the Internet Assigned Numbers Authority (IANA) [11]. For example, 0x06: TCP 0x11: UDP

Table 148. Service Name Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x02	Identifies the sub-attribute
Length	2	1-255	The length in octets of the fields following the length field in the sub-attribute
Service Name	1-255	Variable	As defined in section 1.3.3

Table 149. Name of the Service Instance Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x03	Identifies the sub-attribute
Length	2	Variable	The length in octets of the fields following the length field in the sub-attribute
Name of Service Instance	Variable	Variable	User friendly name of service instance in UTF-8 format. Usually only for public services due to privacy concerns.

Table 150. TextInfo Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x04	Identifies the sub-attribute
Length	2	Variable	The length in octets of the fields following the length field in the sub-attribute
TextInfo	Variable	Variable	TextInfo is used for meta data associated with a service. The content of this field is a sequence of items. Each item starts with an 8-bit length and is followed by the data for the item. The length is the number of bytes of data (excluding the length). The data is text in the format key[=value]. Keys and values follow the rules specified by sections 6.4 and 6.5 of RFC 6763 [12] for TXT records. Keys beginning with "_" are reserved for future use. A key must not be used more than once within a Service Info field.

Table 151. UUID Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x05	Identifies the sub-attribute
Length	2	16	The length in octets of the fields following the length field in the sub-attribute
UUID	16	Variable	A universally unique identifier (UUID) is a 128-bit number used to identify a specific service known to the publisher and the subscriber. Usually used for private services due to privacy concerns.

Table 152. BLOB Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0x06	Identifies the sub-attribute
Length	2	Variable	The length in octets of the fields following the length field in the sub-attribute
BLOB	Variable	Variable	BLOB is used for conveying binary data associate with a service.

Table 153. Vendor Specific Info Sub-attribute format

Field	Size (octets)	Value	Description
Sub-attribute ID	1	0xDD	Identifies the sub-attribute
Length	2	Variable	The length in octets of the fields following the length field in the sub-attribute
OUI	3	Variable	Vendor OUI
Body	Variable	Variable	Vendor Specific body that is implementation specific

9.7 Frame Usage

Table 154 defines the NAN protocol frames that may be transmitted (T) and received (R) by NAN Devices in the different states.

Table 154. NAN Device states and frame usage

	NAN Discovery Beacon frame	NAN Synchronization Beacon frame	NAN Service Discovery frame and Action frames
Master	T, R	T, R	T, R

	NAN Discovery Beacon frame	NAN Synchronization Beacon frame	NAN Service Discovery frame and Action frames
Non-Master Sync	R	T, R	T, R
Non-Master Non-Sync	R	R	T, R

10 Bloom filter creation and use for NAN

10.1 Bloom filter basics

A Bloom filter consists of a bit array of m bits, all initialized to 0, and k different hash functions $h_1,h_2…,h_k$. Each hash function h_i maps an input x to a bit position $b_i(x)$ ($1 <= b_i(x) <= m$).

A Bloom filter represents a set of inputs as follows:

1. Corresponding to each input x, k bit positions $b_1(x),b_2(x),…,b_k(x)$ of which maps or hashes a set element to one of the m array positions with a uniform random distribution.
2. The bits at position $b_1(x),….b_k(x)$ are set to one.

An illustration of a Bloom filter is shown in Figure 64.

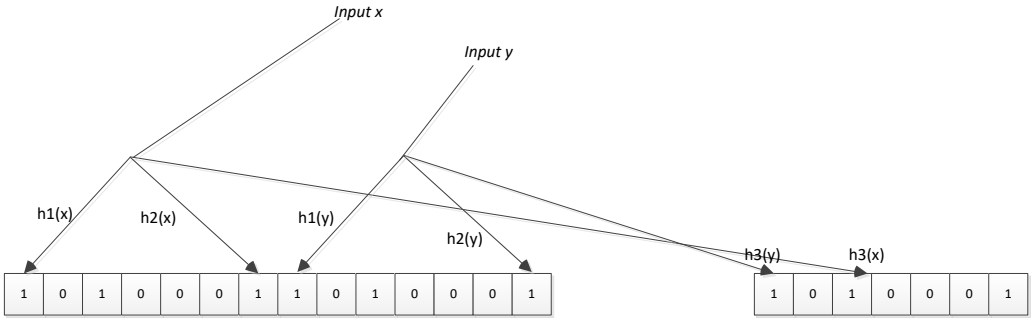


Figure 64. Illustration of a bloom filter

10.2 Hash function for use in NAN

Sixteen hash functions consisting of four sets of four hash functions to be used for hashing the NAN Interface Addresses of frames belonging to a NAN cluster are defined. A single bloom filter is constructed using the four hash functions from the same set. The sets of hash functions are shown in Table 155.

Notation:

H(j,X,M) is hash function of index j for an input X for a bloom filter of length M and is computed as follows. j ranges from 0x00, 0x0F in hex notation.

H(j,X,M) is computed as follows:

1. Compute A(j,X) = [j || X] where j is represented in one byte
2. Compute B(j,X) = CRC32(A(j,X)) & 0x0000FFFF. i.e., obtain the last 2 bytes of the 32-bit CRC of A(j,X)
3. H(j,X,M) = B(j,X) mod M

Table 155. Bloom filter hash functions and index

Set	Bloom Filter Index (Binary)	Hash Functions			
		1	2	3	4
1	00	H(0x00,X,M)	H(0x01,X,M)	H(0x02,X,M)	H(0x03,X,M)
2	01	H(0x04,X,M)	H(0x05,X,M)	H(0x06,X,M)	H(0x07,X,M)
3	10	H(0x08,X,M)	H(0x09,X,M)	H(0x0A,X,M)	H(0x0B,X,M)
4	11	H(0x0C,X,M)	H(0x0D,X,M)	H(0x0E,X,M)	H(0x0F,X,M)

10.2.1 CRC algorithm and bloom filter endian specification

The CRC algorithm used in step 2 in section 10.2 for computing H(j,X,M) shall be taken from [6] as shown in Table 156 and updated to remove the “~0U” operations. An example implementation is shown below.

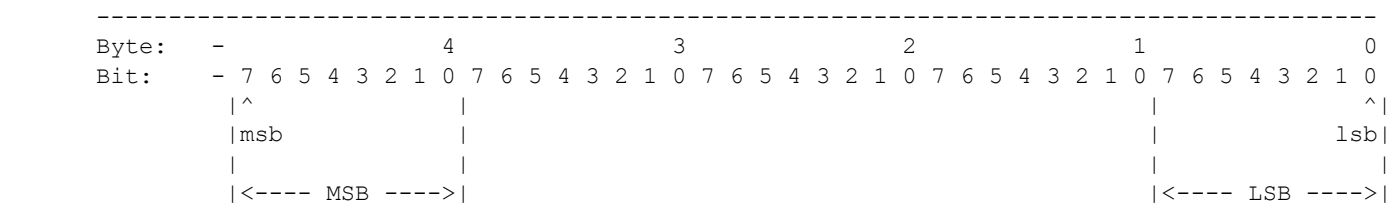
```
uint32_t
crc32(uint32_t crc, const void *buf, size_t size)
{
        const uint8_t *p;
        p = buf;
        while (size--)
               crc = crc32_tab[(crc ^ *p++) & 0xFF] ^ (crc >> 8);
        return crc;
}
```

Table 156. CRC algorithm and Bloom filter variables

Algorithm	Bloom filter variable
crc	Initialized to 0xFFFFFFFF
buf	Input to the bloom filter i.e. A(j,X) shown in section 10.3 buf[0] = j if X = AA:BB:CC:DD:EE:FF, AA is the MSB and FF is the LSB of the MAC Address buf[1] = AA; buf[2] = BB ….buf[6] = FF;
size	Length of input string (7 octets)
crc32_tab	See Appendix G

All CRC operations shall be seeded with the value 0xFFFF_FFFF.

Filter data bytes should be organized with least-significant-bit (LSB) of the least-significant-byte (LSB) as bit 0. For example, consider a Bloom filter of length M = 40 bits. The data shall be arranged as follows:



To find the filter data byte/bit values from the absolute bit positions resulting from the hash computation:

```
uint16_t absBit = H(j, X, M);
uint16_t filterByte = absBit / 8;
uint16_t filterBit = absBit % 8;
```

Then, to set the bit:

```
filterData[byte] |= 1 << absBit;
```

Refer to Appendix F for test cases that may be used for verifying the bloom filter generation.

10.3 Service Response Filter element

At the sender side, the SRF element with a SRF Control field type set to one is generated as follows. Then the Address Set is represented using a Bloom Filter of length M.

Notation:

N = Number of entries to indicate

M = Bloom filter length in bits

The length of the Bloom Filter M shall be chosen to be an integer number of octets and should be chosen to be larger than 5 * N bits. This allows for a false positive probability of ~10% (Note: False positive probability reduces with increasing M, 10*N bits for 1%, 15*N bits for 0.1%). Create the Bloom Filter using one of the sets of Hash functions in section 10.3. Indicate the hash function used in the Bloom Filter Index field for the SRF Control field of the SRF attribute.

False positive probabilities can be further reduced by using different sets of Hash functions in different NAN Service Discovery frames.

At the receiver side, on receiving a NAN Service Discovery frame with SRF attribute type indicating a bloom filter in the Address Set, a receiver performs the following operation to determine if it is a member of the Address Set.

1. Compute the 4-bit positions using the receivers NAN Interface Address and the hash functions corresponding to the index carried in the Bloom Filter index field (refer to Table 155) and the length of received Address Set (M).
2. If the 4-bit position sets computed in step 1 above all have a value of 1, then the receiver's NAN Interface Address is a member of the Address Set.

If a receiver's NAN Interface Address is a member of the Address Set, it responds to the NAN Service Discovery frame based on the Include bit of the SRF Control field within the SDA.

11 Bluetooth Low Energy triggers NAN

Bluetooth Low Energy (BLE) Transport Discovery Service (TDS) may be used to trigger a device to power on its NAN radio for service discovery. The generic frame formats specified in Transport Discovery Service Specification [13] to carry basic service information to trigger further discovery over NAN shall be used.

NOTE: Though the mechanism described in this section is specific to BLE triggering NAN, the same mechanism can be applied to trigger other radios such as Wi-Fi Direct, WiGig, HaLow or those pertaining to infrastructure.

11.1 Frame format

Figure 65 illustrates the BLE TDS frame format used to trigger a NAN radio. The BLE trigger data is encapsulated within the BLE advertising packet with the Transport Discovery Data AD Type Code field set to 0x26 (TDS) and the Organization ID field set to 0x02 (Wi-Fi Alliance Generic Service Discovery).

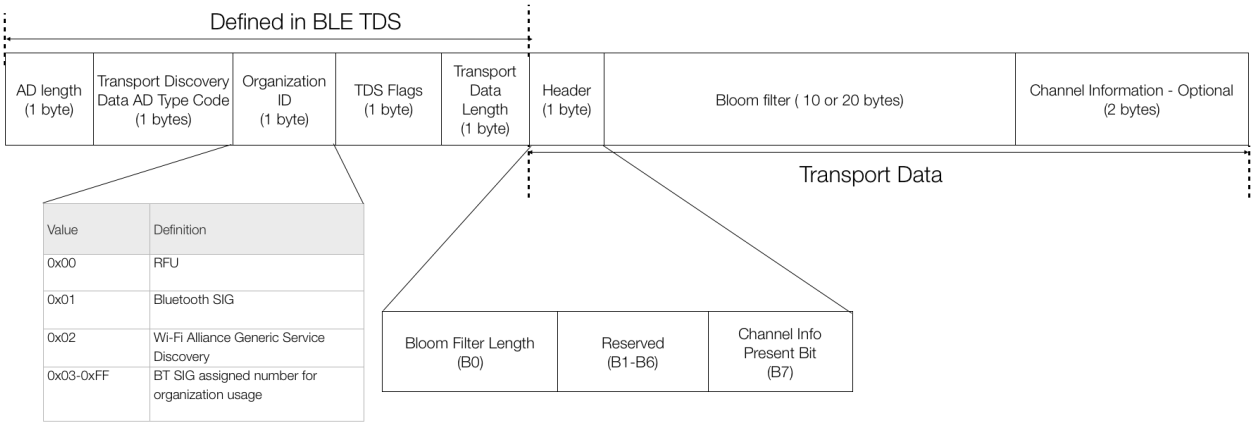


Figure 65. BLE TDS Transport Discovery Data AD Type frame format

The Transport Data field consists of a 1-byte Header field, a variable length Bloom Filter field, and an optional Channel Information field. When generating the content of the Transport Data field, there shall not be any data after the fields defined in section 11.1. When parsing the Transport Data field, any data after the fields defined in section 11.1shall be ignored to allow a future version of this specification to extend the Transport Data field.

The Header field is defined in Table 157.

Table 157. Header field definition

Bits	Subfield name	Description
0	Bloom Filter Length	0b0: The length of the Bloom Filter field is 10 bytes 0b1: The length of the Bloom Filter field is 20 bytes
1-6	Reserved	Reserved for future use
7	Channel Information Present Bit	0b0: The Channel Information field is not present 0b1: The Channel Information field is present.

The Bloom Filter field contains a set of bit positions that are set to 1 after hashing the Bloom Filter elements. The Bloom Filter element is described in section 11.2.

If the Channel Information Present bit is set to 1 in the Header field, then the Channel Information field is included in the BLE TDS frame. If present, the Channel Information field consists of one byte of Operating Class and one byte of Channel Number as defined Annex E of [2]. Inclusion of this field is optional as described in section 11.4.

11.2 Bloom Filter elements

The Bloom Filter elements are case-sensitive text strings describing the services being offered, searches being discovered, and/or the services being activated. The strings shall use the following format:

```
<operation>[;<parameters]:<service name>%<data link identifier>
```

11.2.1 Operations

The Bloom Filter element <operation> string values are defined in Table 158.

Table 158. Operations string values

String	Operation	Description
a	Device-specific activation	Shall include a "bta" parameter defined in section 11.2.2 with the BLE address of the provider device intended to be activated.
b	Browse for a service and request activation the data link if there is a match	Advertised by browsers to indicate they are looking for the specified service. Providers match against this string to determine if an advertisement from a browser is for a service they are providing. This differs from an "s" seek in that Providers activate the data link(s) if there is a match.
p	Provider of a service	Advertised by providers if they received an advertisement from a seeker that matches a service they are providing. Seekers also match against this to determine if an advertisement from a provider is for a service they are seeking.
s	Seek a service without requesting activation the data link on matches	Advertised by seekers to indicate they are seeking the specified service. Providers match against this to determine if an advertisement from a seeker is for a service they are providing. This differs from an "b" browse in that Providers should not activate the data link(s) based only on this match (but may activate based on other matches, e.g. the “a” activation).

11.2.2 Parameters

The Bloom Filter element [;<parameters] string values are defined in Table 159.

Table 159. Parameters string values

String	Parameter	Description
bta	BLE address string	This is the BLE address used in the advertisement packet (i.e. the Private Resolvable Address), not the secret address used to derive the address in the packet. Lowercase, colon-separated string used with activate operation "a" defined in section 11.2.1. For example, 00:11:22:aa:bb:cc.

11.2.3 Service Name

The Service Name in the Bloom Filter element hashed by the Bloom filter shall conform to the Service Name definition in Table 1.

11.2.4 Data link identifier

The data link identifiers are text strings to indicate the data link being offered or requested and shall be prefixed by "%".

For NAN, the data link identifier is set to “nan”.

11.2.5 Bloom Filter element examples

In the following examples, “_ipp._tcp” is used as the Service Name.

For a Seeker to discover an ipp service over NAN, it would advertise:

```
s:_ipp._tcp%nan
```

For a Browser to discover an ipp service over NAN, it would advertise:

```
b:_ipp._tcp%nan
```

For a Provider to respond to a Seeker's or Browser's advertisement, it would include:

```
p:_ipp._tcp%nan
```

For a Seeker to activate the NAN interface of the device that advertised from the BLE address 11:22:33:aa:bb:cc, it would advertise:

```
a;bta=11:22:33:aa:bb:cc:_ipp._tcp%nan
```

This string would also be included by the provider after its data link was activated.

11.2.6 False positives

A Bloom filter is a probabilistic data structure that does not generate a false negative but may generate a false positive. The probability of a false positive increases with the number of Bloom filter elements. The estimated probability of a false positive for different numbers of services over the entire set of possible elements is given below.

10-byte Bloom filter:

- 5 services: 0.239%
- 10 services: 2.397%
- 20 services: 15.966%
- 30 services: 36.424%

20-byte Bloom filter:

- 5 services: 0.019%
- 10 services: 0.239%
- 20 services: 2.397%
- 30 services: 7.750%

11.2.7 ABNF

The following defines the Augmented Backus-Naur Form (ABNF) as defined by RFC 5234 [14] for each Bloom Filter element.

```
Element        = op *(";" 1(opParam)) ":" serviceType "%" dataLinkID
   op            =/ "a" ; Activate data link. Requires bta.
   Op            =/ "p" ; Provide service.
   Op            =/ "s" ; Seeker of service.
   opParam       =/ "bta=" bta
   bta           = 2HEXDIG 5( ":" 2HEXDIG )
   serviceType   = UTF8-octets ; Per RFC 6335 section 5 [15]
   dataLinkID    = UTF8-octets
```

11.3 Bloom filter generation

Generating the Bloom filter uses SipHash [16] with a fixed key of "00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01" and a hash count of 4. SipHash generates a 64-bit hash, therefore a single invocation provides enough randomness for all four hashes. The first bit index uses the 64-bit SipHash result mod bitCount, where bitCount is the number of bits for a 10-byte or 20-byte Bloom filter. The result is divided by bitCount and then mod with bitCount to generate the second bit index, and so on to generate all 4-bit indexes. The resulting bits are set to form the Bloom filter.

The following C code demonstrates how to generate the Bloom Filter.

```
#define kTDSSipHashKey ( (const uint8_t *) \
    "\x00\x00\x00\x00\x00\x00\x00\x00" \
    "\x00\x00\x00\x00\x00\x00\x00\x01" \
    )

#define kTDSSipHashCount        4

void
    TDSBloomFilterAddString(
        uint8_t *       inFilterPtr,
        size_t          inFilterLen,
        const char *    inStr,
        size_t          inLen )
{
    const size_t bitCount = inFilterLen * 8;
    uint64_t hash = SipHash( kTDSSipHashKey, inStr, inLen );
    for( uint8_t i = 0; i < kTDSSipHashCount; ++i )
    {
        const size_t idx = hash % bitCount;
        inFilterPtr[ idx / 8 ] |= ( 1 << ( 7 - ( idx & 7 ) ) );
        hash /= bitCount;
    }
}

bool
    TDSBloomFilterContainsHash(
        const uint8_t * inFilterPtr,
        size_t          inFilterLen,
        uint64_t        inHash )
{
    const size_t bitCount = inFilterLen * 8;
    for( uint8_t i = 0; i < kTDSSipHashCount; ++i )
    {
        const size_t idx = inHash % bitCount;
        const uint8_t on = inFilterPtr[ idx / 8 ] &
            ( 1 << ( 7 - ( idx & 7 ) ) );
        if( !on ) return( false );
        inHash /= bitCount;
    }
    return( true );
}

bool
    TDSBloomFilterContainsString(
        const uint8_t * inFilterPtr,
        size_t          inFilterLen,
        const char *    inStr,
        size_t          inLen )
{
    const uint64_t hash = SipHash( kTDSSipHashKey, inStr, inLen );
    return( TDSBloomFilterContainsHash( inFilterPtr, inFilterLen,
        hash ) );
}
```

11.4 Protocol flow

Figure 66 shows the protocol flow for both the Provider of a service and a Browser of the service at different phases during the discovery process.

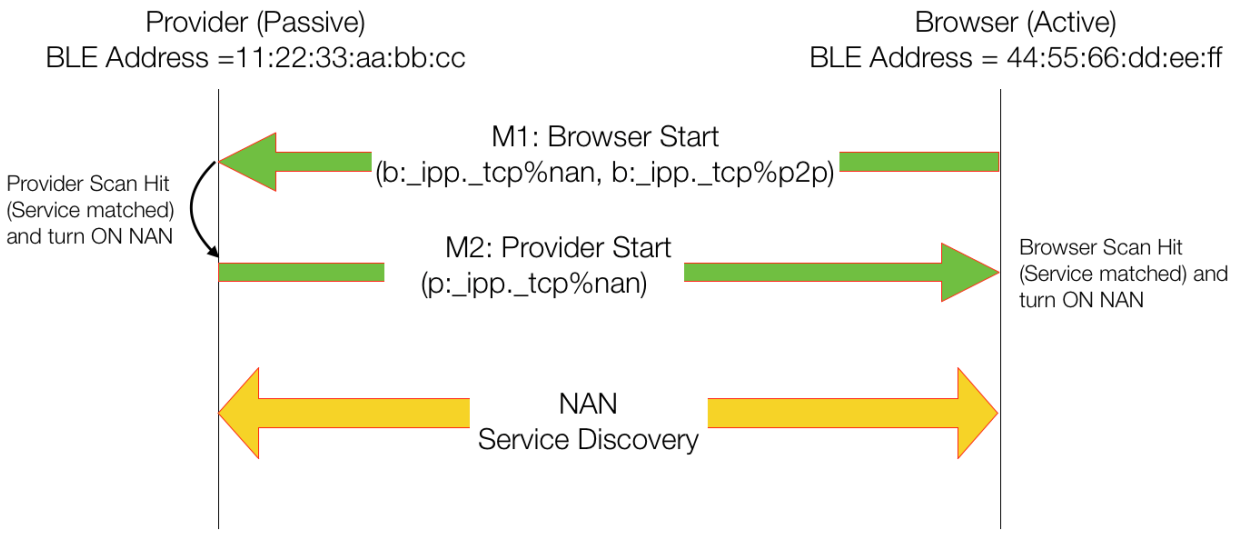


Figure 66. Example of protocol flow for BLE triggers NAN operation initiated by a Browser

Figure 67 shows the protocol flow for both the Provider of a service and a Seeker of the service at different phases during the discovery process.

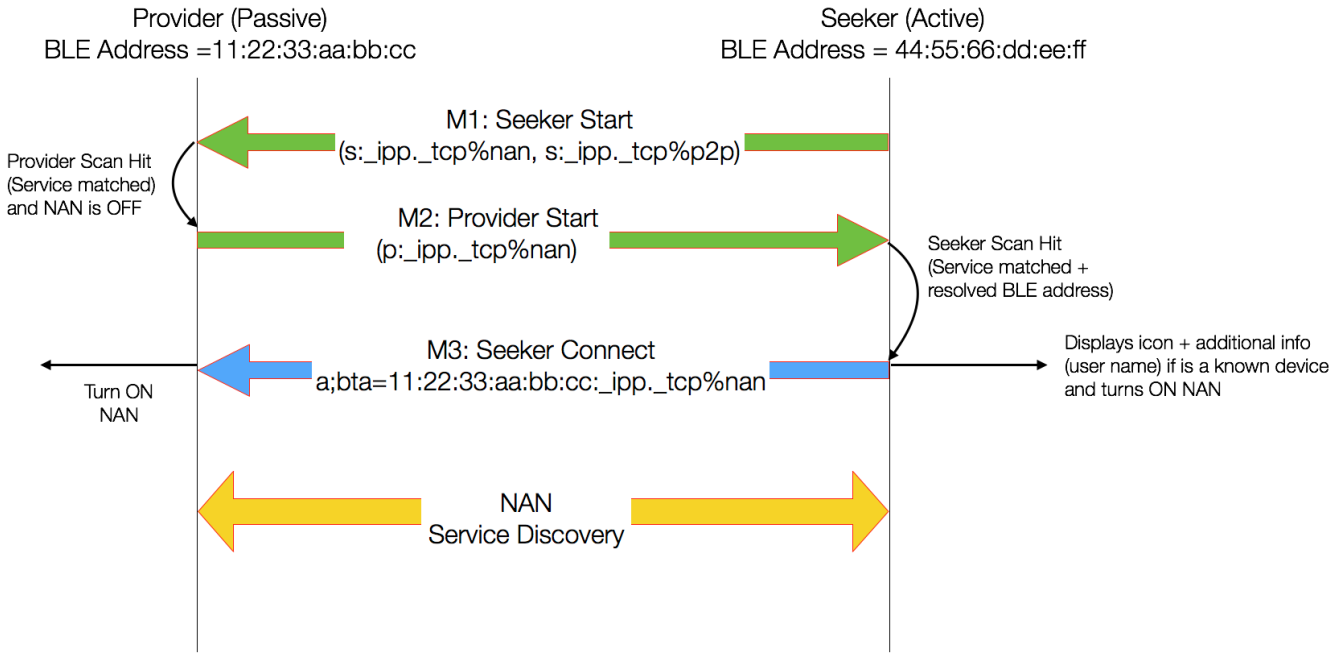


Figure 67. Example of protocol flow for BLE triggers NAN operation initiated by a Seeker

It is important to note that the BLE triggered NAN operations are isochronous protocols whereby advertisements during each phase are not a one-time advertisement. The advertisements shall be repeated until a peer's advertisement satisfy the request, the user cancels, or a timeout occurs. Phases for different operations may overlap. For example, a Seeker may be looking for "p:_ipp._tcp" (phase 1) and bringing up another service "a:bta=11:22:33:44:55:66:_airdrop._tcp" (phase 3) at the same time. Both operations may be merged into the same advertisement packet.

11.4.1 General rules

1. On/Off status indication via Transport State subfield in the BLE TDS Packet:
   a. The Seeker/Provider shall only set the Transport State subfield to 01 in the TDS Flags field indicating an "On" status when all the data link identifiers present in the Bloom Filter element are on. Otherwise, the Transport State subfield shall be set to 00 indicating an "Off" status.

2. Channel Information inclusion via Channel Information Present Bit in the BLE TDS Packet:
    a. The Seeker/Provider may include the Channel Information field by setting the Channel Information Present Bit in the header to 1, when only one data link identifier is present in the Bloom Filter element.
    b. The Seeker/Provider shall not include the Channel Information field by setting the Channel Information Present Bit in the header to 1 when multiple data link identifiers are present in the Bloom Filter element.

11.4.2 Operation phases

Phase 1:

A Browser or Seeker shall start to advertise with non-connectable, undirected advertising (i.e., ADV_NONCONN_IND denoted as an M1 message) containing the searched services. The Browser or Seeker shall set Channel Information Present Bit and set the Transport State subfield according to the rules in section 11.4.1.

Phase 2:

When an M1 is received by a Provider, the Provider shall check if there is a match in the Bloom filter.

1. If there is no match, the Provider shall ignore the M1.
2. If there is a "s" seek match, the Provider shall advertise with a ADV_NONCONN_IND (denoted as an M2) containing the matched services. The Provider may also include other supported services in the M2 message. The Provider should not turn on its NAN radio and shall set the Channel Information Present Bit and set the Transport State subfield according to the rules in section 11.4.1.
3. If there is a “b” browse match, the Provider shall advertise with a ADV_NONCONN_IND (denoted as an M2) containing the matched services. The Provider may also include other supported services in the M2 message. The Provider shall turn on its NAN radio, set the Channel Information Present Bit, and set the Transport State subfield according to the rules in section 11.4.1.

Phase 3:

When an M2 message is received by a Browser, the Browser shall check if there is a match in the Bloom filter.

1. If there is no match, the Browser shall ignore the M2.
2. If there is a match, the Browser shall turn on its NAN radio and start NAN discovery as described in sections 3 and 4.

When an M2 message is received by a Seeker, the Seeker shall check if there is a match in the Bloom filter.

1. If there is no match, the Seeker shall ignore the M2.
2. If there is a match and if the Seeker decides to select a specific Provider, then the Seeker shall advertise with a ADV_NONCONN_IND (denoted as an M3) containing the matched services and the Provider’s BLE address. The Seeker may also include other supported services in the M3 message. This M3 message serves as a trigger for that specific Provider (via its BLE address) to turn on its NAN radio. The Seeker shall turn on its NAN radio and start NAN discovery, set the Channel Information Present Bit, and set the Transport State subfield according to the rules in section 11.4.1.

Phase 4:

When an M3 message is received by a Provider, the Provider shall check if there is a match in the Bloom filter.

1. If there is no match, the Provider shall ignore the M3.
2. If there is a match, the Provider shall turn on its NAN radio to start NAN discovery as described in sections 3 and 4.

12 NAN Operations triggered by NFC

NOTE: THIS FEATURE HAS NOT BEEN TESTED IN THE Wi-Fi Aware CERTIFICATION PROGRAM.

NAN Devices with NFC radios may use the NFC Connection Handover protocol [17] to trigger NAN service discovery and secured NDP setup.

12.1 NFC Negotiated Connection Handover

A NAN Device pair that supports the NFC Negotiated Connection Handover may select an NCS-PK-2WDH cipher suite and use the NFC communication to conduct the two-way authenticated Diffie–Hellman key exchange. The successful completion of the NFC Negotiated Connection Handover enables the pair of devices to obtain each other's DH Public Key and other trigger information.

The NFC triggered NCS-PK-2WDH is conducted by using the NFC Negotiated Connection Handover protocol. An NFC Handover Requester transmits an NFC Handover Request message to an intended NFC Handover Selector. The NFC Handover Selector responds with an NFC Handover Select message to the NFC Handover Requester to complete the negotiated handover process. If handover to Wi-Fi Aware is selected, both devices shall turn on NAN radios and start NAN discovery.

NOTE: Either the NAN Service Subscriber or Publisher may serve as the NFC Handover Requester.

Figure 68 shows an example of the NFC triggered NAN protocol using the NFC Negotiated Connection Handover, with the NAN Service Subscriber serving as the NFC Handover Requester.

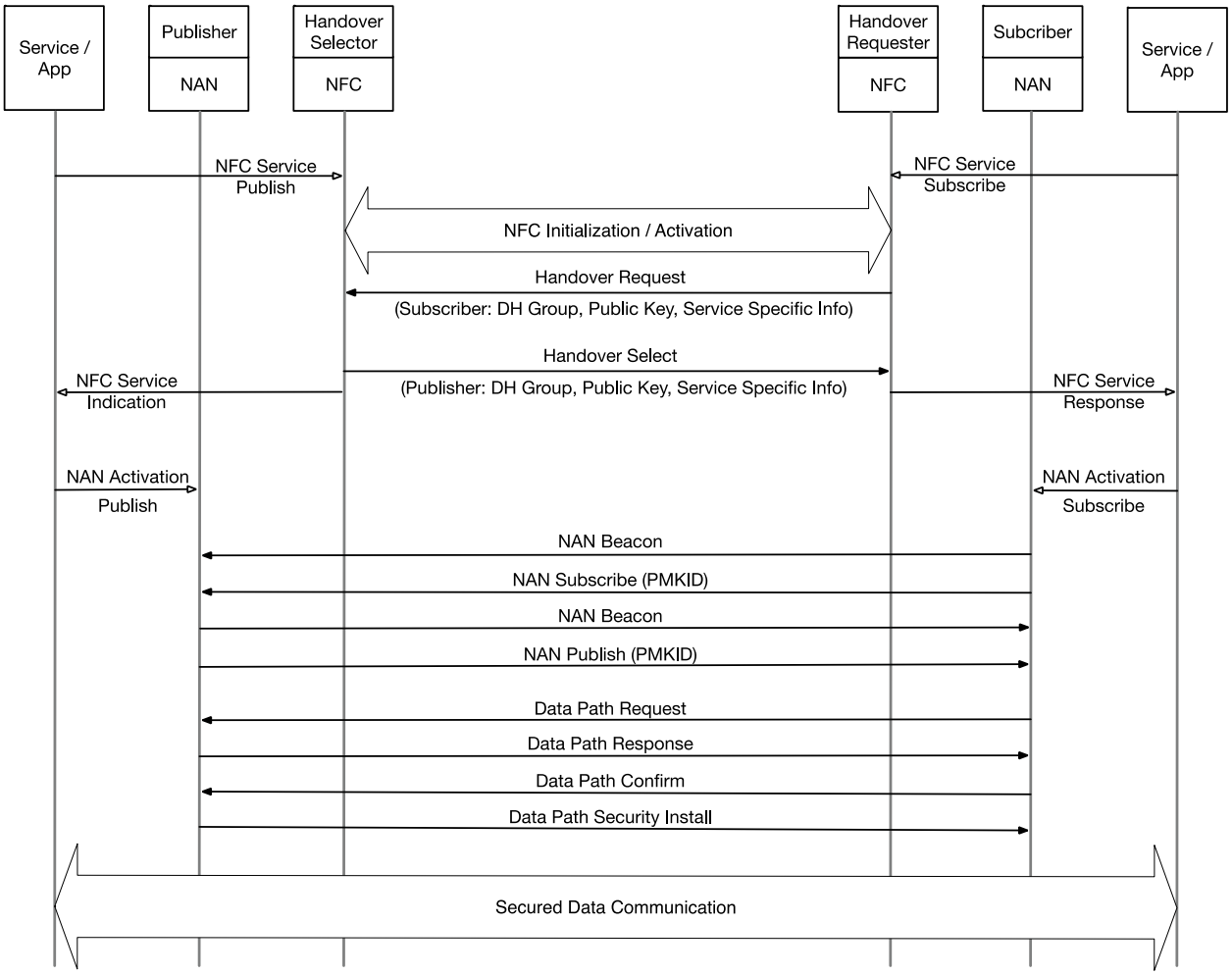


Figure 68. Example of NFC triggered NAN Protocol using NFC Negotiated Connection Handover with Service Subscriber serving as NFC Handover Requester

The NFC Handover Request message format is shown in Figure 69, and the Handover Request Record format is shown in Table 160.

If an NFC Handover Requester supports handover to Wi-Fi Aware for a service, it shall include the Wi-Fi "ac" Record in the Handover Request Record, and shall also include the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Request message. The service specific information is included in the Aux Record, which associates to one or multiple handover carriers. The definition of the Aux Record format is out of the scope of this specification.

Figure 69. NFC Handover Request Message Format

Table 160. Handover Request Record

Field	Size (Octet)	Sub-Field	Value
HDR	1	Header	0x91 (MB=1, ME=0, CF=0, SR=1, IL=0, TNF=001b)
	1	Type Length	0x02
	1	Payload Length	0x11 (if zero Aux Ref record) or 0x13 (if one Aux Data Ref record)
	2	Type	0x48, 0x72: “Hr” (Well Known Global Type - Handover Request)

Field	Size (Octet)	Sub-Field	Value
Version	1	Version	0x15 (NFC Connection Handover Specification 1.5)
CR Record	1	Header	0x91 (MB=1, ME=0, CF=0, SR=1, IL=0, TNF=001b)
	1	Type Length	0x02
	1	Payload Length	0x02
	2	Type	0x63, 0x72: “cr” (Well Known Local Type - Collision Resolution)
	2	Payload	2-byte Random Number
Wi-Fi "ac" Record	1	Header	0x51 (MB=0, ME=1, CF=0, SR=1, IL=0, TNF=001b)
	1	Type Length	0x02
	1	Payload Length	0x04 (if zero Aux Ref record) or 0x06 (if one Aux Data Ref record)
	2	Type	0x61, 0x63: “ac” (Well Known Local Type - Alternate Carrier)
	1	Carrier Power State	0x01 (Active)
	1	Carrier Data Ref Length	0x01
	1	Carrier Data Ref Value	0x57: "W" (ID of Wi-Fi Aware Carrier Configuration Record)
	1	Aux Data Ref Count	0x00 (if zero Aux Ref record) or 0x01 (if one Aux Data Ref record)
	1	Aux Data Length	0x01
	1	Aux Data Ref Value	0x41: "A" (ID of Service Specific Data e.g. a Verb record)

The format of the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Request message is shown in Table 161.

The NFC Handover Requester shall include the Cipher Suite Info field with one or multiple NAN Cipher Suite IDs in the Wi-Fi Aware Carrier Configuration Record to indicate the supported NAN cipher suite(s). If the NFC Handover Requester supports an NCS-PK-2WDH cipher suite, it shall include at least one DH Info field in the Wi-Fi Aware Carrier Configuration Record to indicate the supported Diffie-Hellman (DH) parameters, which include the DH Key Group and the corresponding DH Public Key. The NFC Handover Requester may include multiple DH Info fields in the Wi-Fi Aware Carrier Configuration Record to indicate the support of multiple DH Key Groups. The NFC Handover Requester shall also include a Band Info field in the Wi-Fi Aware Configuration Record to indicate the supported NAN operating band(s).

The Channel Info field serves as a placeholder for future extension, and may optionally be included in the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Request message.

Table 161. Wi-Fi Aware Carrier Configuration Record "W"

Field	Size (Octet)	Sub-Field	Value
HDR	1	Header	0x1A or 0x5A: (MB=0, ME=0 or 1, CF=0, SR=1, IL=1, TNF=010b) Value of ME depends on availability of the subsequent Aux Data Record(s).
	1	Type Length	0x17
	1	Payload Length	Variable
	1	ID Length	0x01
	23	Type	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x77 0x66 0x61 0x2E 0x6E 0x61 0x6E Media Type RFC 2046: “application/vnd.wfa.nan”
	1	ID	0x57: "W" (Record ID)
Cipher Suite Info	1	Length	Variable

Field	Size (Octet)	Sub-Field	Value
	1	Data Type	0x01
	Variable	Cipher Suite ID Info	A list of supported NAN cipher suites, or a selected NAN cipher suite. Each Cipher Suite ID occupies one octet.
DH Info	1	Length	Variable
	1	Data Type	0x02
	2	DH Key Group	Variable Specified at: https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8
	Variable	DH Public Key	Variable (length / contents vary with DH Key Group Type)
Pass-phrase Info	1	Length	Variable
	1	Data Type	0x03
	Variable	Pass-phrase	Variable
Band Info	1	Length	0x02
	1	Data Type	0x04
	1	Supported Bands	Bitmap: Bit 0: Reserved (for TV white spaces) Bit 1: Sub-1 GHz (excluding TV white spaces) Bit 2: 2.4 GHz Bit 3: Reserved (for 3.6 GHz) Bit 4: 4.9 and 5 GHz Bit 5: Reserved (for 60 GHz) Bit 6: Reserved (for 45 GHz) Bit 7: 6 GHz
Channel Info	1	Length	0x03
	1	Data Type	0x05
	1	Operating Class	Variable Specified at: Table E-4 Global Operating Classes in Annex E of [19].
	1	Channel Number	Variable
Vendor Specific Info	1	Length	Variable
	1	Data Type	0xDD
	3	OUI	Variable Vendor OUI
	Variable	Value	Variable

If an NFC Handover Selector selects Wi-Fi Aware as the handover carrier for a service, it shall include the Wi-Fi "ac" Record in the Handover Select Record of the NFC Handover Select message, and shall also include the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message. The service specific information is included in the Aux Record.

The NFC Handover Select message format is shown in Figure 70, and the Handover Select Record format is shown in Table 162.

Figure 70. NFC Handover Select Message Format

Table 162. Handover Select Record

Field	Size (Octet)	Sub-Field	Value
HDR	1	Header	0x91(MB=1, ME=0, CF=0, SR=1, IL=0, TNF=001b)
	1	Type Length	0x02
	1	Payload Length	0x0A (if zero Aux Ref record) or 0x0C (if one Aux Data Ref record)
	2	Type	0x48, 0x73: “Hs” (Well Known Global Type - Handover Select)
Version	1	Version	0x15
Wi-Fi "ac" Record	1	Header	0xD1 (MB=1, ME=1, CF=0, SR=1, IL=0, TNF=001b)
	1	Type Length	0x02
	1	Payload Length	0x04 (if zero Aux Ref record) or 0x06 (if one Aux Data Ref record)
	2	Type	0x61, 0x63: “ac” (Well Known Local Type - Alternate Carrier)
	1	Carrier Power State	0x01 (Active)
	1	Carrier Data Ref Length	0x01
	1	Carrier Data Ref Value	0x57: "W" (ID of Wi-Fi Aware Carrier Configuration Record)
	1	Aux Data Ref Count	0x00 (if zero Aux Ref record) or 0x01 (if one Aux Data Ref record)
	1	Aux Data Length	0x01
	1	Aux Data Ref Value	0x41: "A" (ID of Service Specific Data e.g. a Verb record)

The format of the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message is the same as that in the NFC Handover Request message, which is shown in Table 161.

The NFC Handover Selector shall include the Cipher Suite Info field with a single Cipher Suite ID in the Wi-Fi Aware Carrier Configuration Record to indicate the selected NAN cipher suite. If the NFC Handover Selector selects an NCS-PK-2WDH cipher suite, it shall include a single DH Info field in the Wi-Fi Aware Carrier Configuration Record to indicate the selected DH parameters, which include the selected DH Key Group and the corresponding DH Public Key. The NFC Handover Selector shall also include a Band Info field in the Wi-Fi Aware Configuration Record to indicate the supported NAN operating band(s).

The Channel Info field serves as a placeholder for future extension, and may optionally be included in the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message.

After a NAN Device pair obtains each other's DH parameters via the NFC Negotiated Connection Handover, they shall use the algorithms specified in [18] to derive a ND-PMK and the corresponding ND-PMKID.

When the NAN Device pair turn on NAN radios and start NAN service discovery, they shall include the derived PMKID in the transmitted Publish or Subscribe messages.

Once the Service Subscriber receives a Publish message from the peer with a service match and ND-PMKID match, the Service Subscriber initiates the secured NDP setup, as specified in section 7.1.3.6.

12.2 NFC Static Connection Handover

A NAN Device pair that supports the NFC Static Connection Handover may select a pass-phrase based NAN cipher suite, such as NCS-SK, and use the NFC communication to convey a pass-phrase and other trigger information from one NAN Device to an intended peer.

An NFC Handover Requester reads an NFC Handover Select message from an intended NFC Handover Selector. If the NFC Handover Select message indicates handover to Wi-Fi Aware, both devices shall turn on NAN radios and start NAN discovery.

NOTE: Either the NAN Service Subscriber or Publisher may serve as the NFC Handover Requester.

Figure 71 shows an example of the NFC triggered NAN protocol using NFC Static Connection Handover, with the NAN Service Subscriber serving as the NFC Handover Requester.

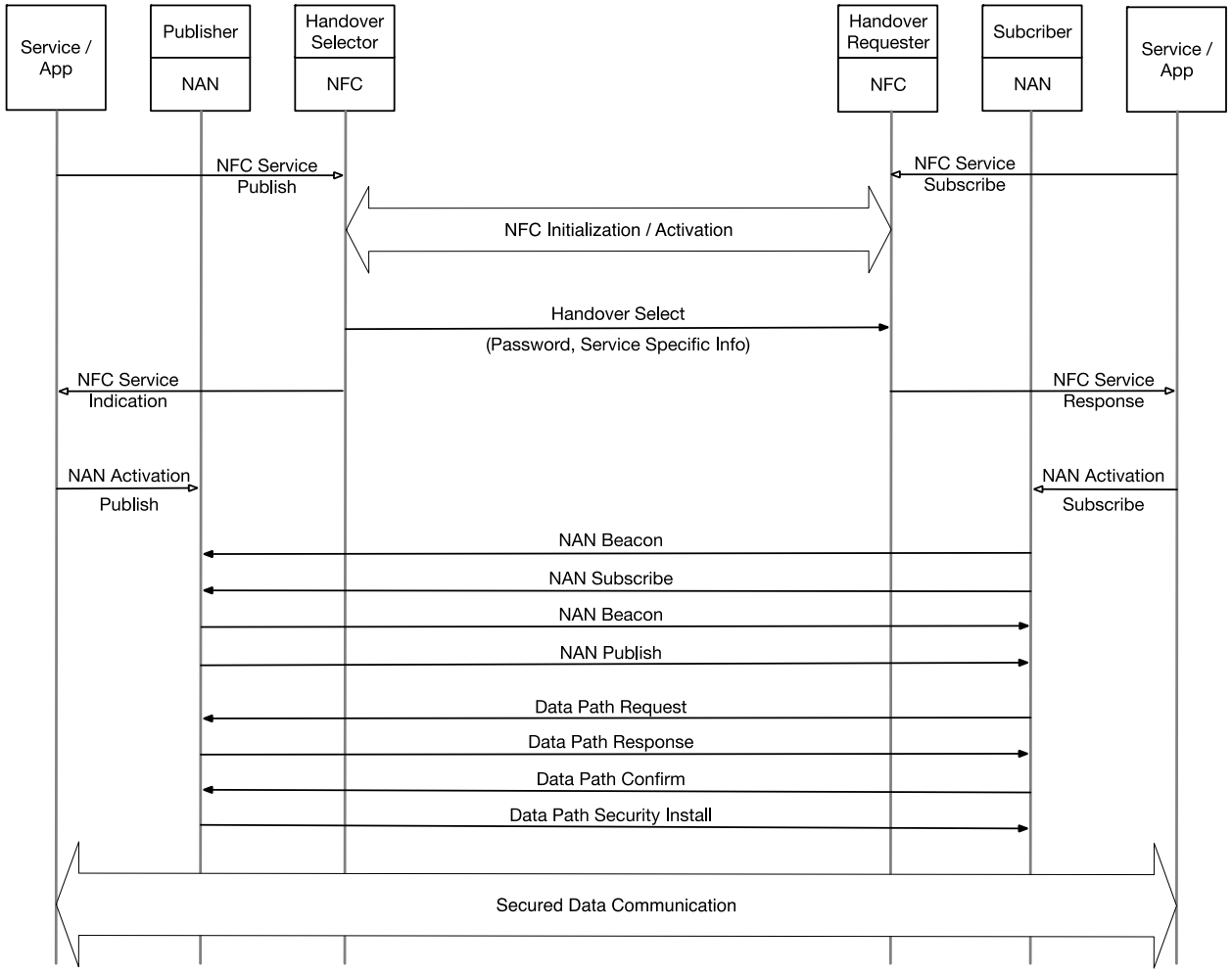


Figure 71. Example of NFC triggered NAN using NFC Static Connection Handover with NAN Service Subscriber serving as NFC Handover Requester

If an NFC Handover Selector selects Wi-Fi Aware as the handover carrier for a service, it shall include the Wi-Fi "ac" Record in the Handover Select Record of the NFC Handover Select message, and shall also include the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message. The service specific information is included in the Aux Record.

The NFC Handover Select message format is shown in Figure 70, and the Handover Select Record format is shown in Table 162. The format of the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message is shown in Table 161.

The NFC Handover Selector shall include the Cipher Suite Info field with one or multiple NAN Cipher Suite IDs in the Wi-Fi Aware Carrier Configuration Record to indicate the supported NAN cipher suite(s). If the NFC Handover Selector indicates an NCS-SK cipher suite, it shall include a Pass-phrase Info field in the Wi-Fi Aware Carrier Configuration Record to specify the selected pass-phrase for the supported cipher suite. The NFC Handover Selector shall also include a Band Info field in the Wi-Fi Aware Configuration Record to indicate the supported NAN operating band(s).

The Channel Info field serves as a placeholder for future extension, and may optionally be included in the Wi-Fi Aware Carrier Configuration Record in the NFC Handover Select message.

After the NFC Static Connection Handover to Wi-Fi Aware is completed, the NAN Device pair shall turn on NAN radios and start NAN service discovery. Once the NAN Service Subscriber receives a Publish message from the NAN Service Publisher with a service match, the NAN Service Subscriber initiates the secured NDP setup, as specified in section □.

If an NCS-SK cipher suite is used, the pass-phrase shall be mapped to a ND-PMK using PBKDF2, as specified in Appendix M.

13 NAN Instant Communication

To support services that require very fast service discovery and data communication, a NAN Device may enable an Instant Communication mode. A NAN Device may enter the Instant Communication mode when triggered by an OOB manner, such as NFC, BLE, or a user operation.

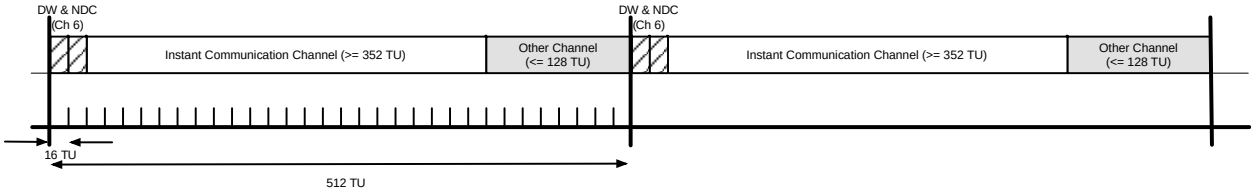


Figure 72. Availability Schedules for Instant Communication

Once a NAN Device enters the Instant Communication mode, and before it exits the mode:

- The NAN Device shall stay awake all the time
- The NAN Device shall follow and indicate the availability schedules as shown in Figure 72
  - The NAN Device shall be present at each 2.4 GHz DW and the default NDC slot on the 2.4GHz NAN Discovery Channel (channel 6)
  - Immediately following the default NDC slot on channel 6, the NAN Device should be present on an Instant Communication Channel and should maximize its presence on the Instant Communication Channel till the next 2.4 GHz DW. The Instant Communication Channel should be one of the NAN Discovery Channels, based on the NAN Device's band capability, an intended peer's band capability (if known), as well as the local regulations. If both the NAN Device and an intended peer are aware of each other's band capabilities and both support 5 GHz band, the Instant Communication Channel should be one of the 5 GHz NAN Discovery Channels, according to section 3.2; otherwise, the Instant Communication Channel should be the 2.4 GHz NAN Discovery Channel (channel 6)
  - After staying at the Instant Communication Channel for at least 352 TU, the NAN Device may switch to a channel different from the Instant Communication Channel until the next 2.4 GHz DW
- The NAN Device shall start to transmit NAN Discovery Beacons outside DWs with a beacon interval between 50 TUs and 200 TUs on the Instant Communication Channel, immediately after it switches to the Instant Communication Channel, and disregarding its roles and states. The NAN Device may skip transmission of NAN Discovery Beacons on a NAN Discovery Channel different from the Instant Communication Channel
- If the NAN Device serves as the Publisher of a service that requires instant communication, it shall include the corresponding Service ID in the Service ID List attribute within the transmitted NAN Beacons. If the NAN Device receives a NAN Beacon from a peer with matched Service ID in the Subscribe Service ID List attribute, it shall transmit a Publish message to the peer
- If the NAN Device serves as the Subscriber of a service that requires instant communication, it shall include the corresponding Service ID in the Subscribe Service ID List attribute within the transmitted NAN Beacons. If the NAN Device receives a NAN Beacon from a peer with matched Service ID in the Service ID List attribute, it shall transmit a Subscribe message to the peer
- When the NAN Device establishes an NDP/NDL with a peer to support a service that requires instant communication, it shall propose the NDL schedule as shown in Figure 72

Figure 73 shows an example of accelerated NAN service discovery when both the Publisher and Subscriber enter the Instant Communication mode.

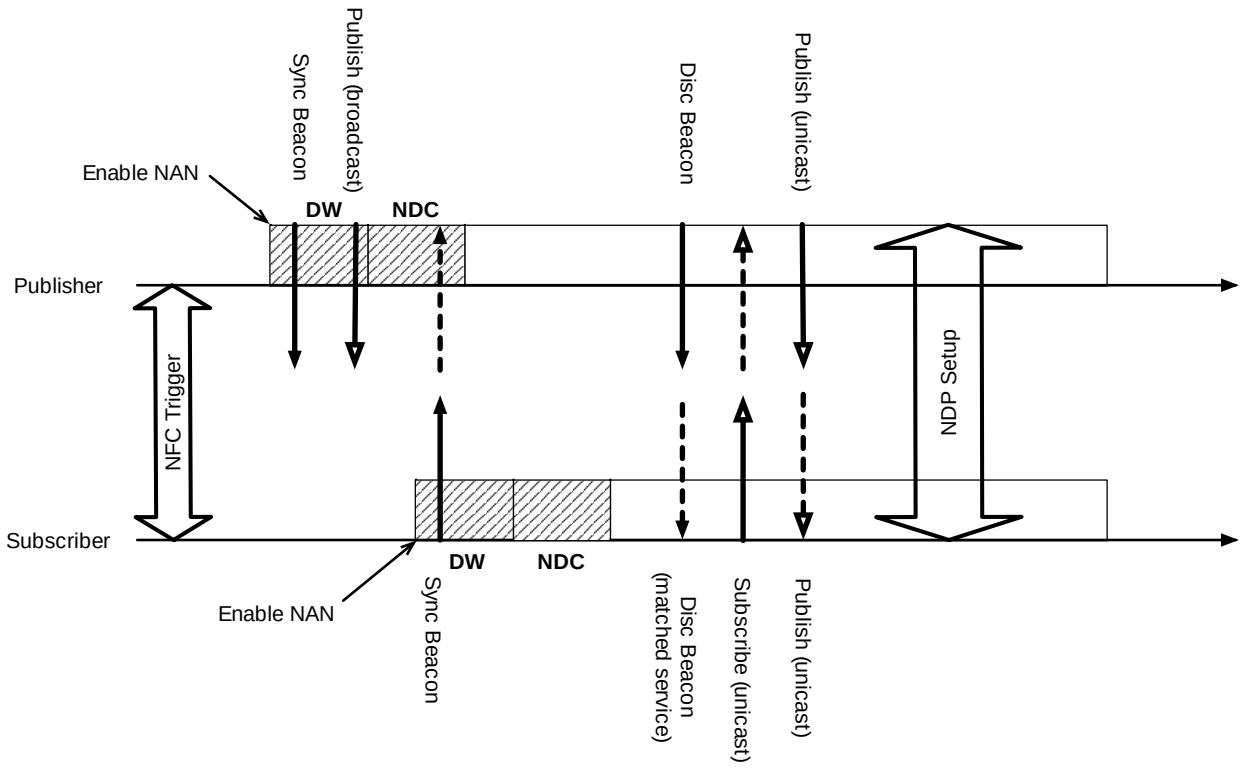


Figure 73. An Example of Accelerated Service Discovery in Instant Communication Mode

The NAN Device exits the Instant Communication mode when the service transaction is completed or when the Instant Communication mode times out, or when the Instant Communication mode is canceled by the NAN Device. How a NAN Device exits the Instant Communication mode is implementation specific.

A NAN Device in the Instant Communication mode shall follow the NAN synchronization and service discovery operations within DWs as specified in section 3 and 4, to ensure interoperability with a peer not entering the Instant Communication mode.

Appendix A (Informative) Post NAN Discovery procedure with P2Ps-ASP

The P2Ps-ASP (Peer to Peer services application service protocol) session setup is the procedure by which a device establishes a P2Ps session with another device following NAN discovery.

The P2Ps-ASP session setup may be performed if the publishing device and subscribing device both support P2Ps. A NAN Device indicates support for P2Ps in the NAN Connection Capability attribute included in the NAN Service Discovery frames.

A.1 P2Ps-ASP Service Discovery procedure using Probe Request and Probe Response frames

To allow for P2Ps setup, a NAN device includes in NAN Service Discovery frames:

- The NAN Connection Capability attribute to indicate that this device is P2Ps capable
- The P2P Operation attribute or Extended P2P Operation attribute to declare the P2P Device operation parameters for P2Ps set up

After NAN Discovery, the device that supports P2Ps and wants to start a P2Ps service session with Advertiser/Publisher calls the SeekService method, as defined by the P2Ps Technical Specification [3] to perform P2Ps-ASP Discovery. At the channel and time declared in the P2P Operation attribute or Extended P2P Operation attribute and NAN Availability attribute, the SeekService method performs Probe Request and Probe Response exchange and optionally performs P2P Service Discovery Request and Response. The Probe Request and Probe Response mechanism is to determine a device that supports the service being seeked. Service Discovery request and response frames are used to get more details about the service being seeked. After NAN Discovery and P2Ps-ASP Discovery, if the device wants to setup a P2Ps service session with remote devices, the device calls the ConnectSessions method to start a session setup including a P2P connection as defined in [3]. Figure 74 illustrates this procedure.

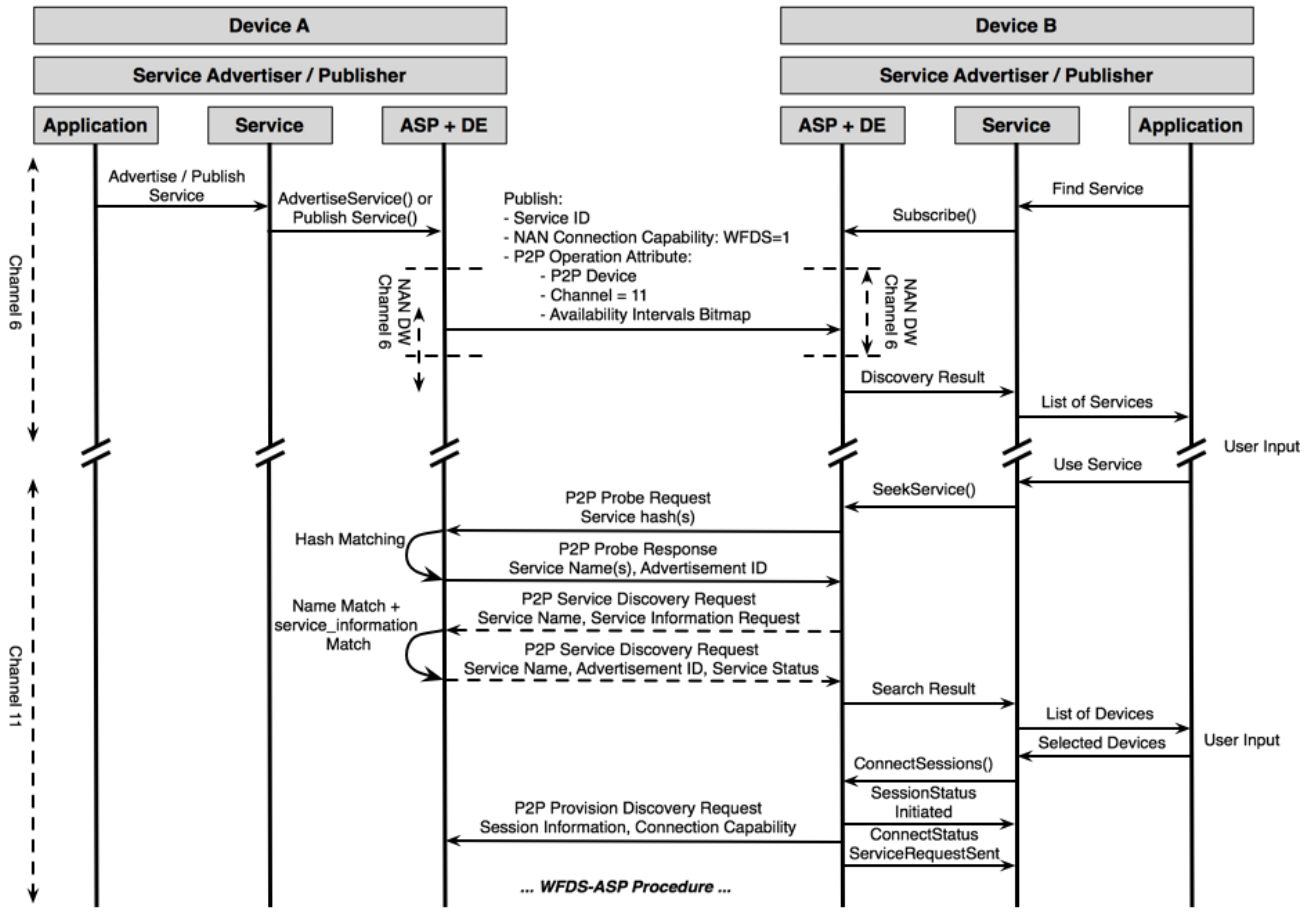


Figure 74. P2Ps-ASP procedure using Probe Request and Probe Response frames

Appendix B (Informative) Recommended practices for transmission of NAN Discovery Beacon frames

While the exact times when a Master device transmits NAN Discovery Beacon frames is implementation specific, this section documents two independent guidelines for the transmission of NAN Discovery Beacon frames that may decrease the time and power required by a scanning device to discover a particular NAN cluster.

The first recommendation consists of having a Master device sending NAN Discovery Beacon frames using a pre-defined time reference that is shared with scanning devices. One such pre-defined time reference is the TSF timer advertised by surrounding Wi-Fi Access Points, which can be used in the following way:

- The Master device can discover the TSF timer of surrounding APs acting in the NAN in 2.4 GHz or 5 GHz channels by receiving Probe Response frames or Beacon frames from these APs
- Among the discovered APs, the Master device selects the AP with the lowest BSSID, and transmits a NAN Discovery Beacon frame when the lower 17 bits of the selected AP's TSF timer are equal to zero
- A scanning NAN device follows the same procedure to discover surrounding APs, selects the AP with the lowest BSSID, and wakes up for a short time around the time when the lower 17 bits of the selected AP's TSF timer are equal to zero

The previous method allows reducing the duration of passive scanning and saving power in the scanning device. However, this method alone does not guarantee that a NAN Device doing passive scanning will discover all its surrounding NAN Clusters, because Master Devices in other NAN Clusters may not follow this guideline or the scanning and the Master device may not be able to see the same AP. Therefore, this guideline is only recommended in implementations where the scanning device can rely on the transmitting behavior of the Master device, and when it is reasonable to assume that both devices will be able to see the same set of APs. To achieve a reliable discovery of NAN Clusters a NAN Device could interleave this method with longer passive scanning durations.

The second recommendation refers to the case of a NAN Cluster where various devices act as Master simultaneously, and consists of avoiding the synchronization of the transmission times of NAN Discovery Beacon frames from different Masters. A possible implementation of this recommendation is to have a Master device introduce a random delay between a Discovery Window and the transmission time of its next NAN Discovery Beacon frame. Thus, the NAN Discovery Beacon frames sent by different Master devices is scattered in time that helps scanning devices to discover the NAN Cluster.

Appendix C (Informative) Recommended practices for selecting a Master Preference value

Selecting the value carried in the Master Preference attribute is an implementation decision. However, the following criteria are recommended to select its value:

- A device with large battery capacity, or plugged into power, should select a high Master Preference value
- A device with good clock stability should select a high Master Preference value
- A moving device should select a low Master Preference value

NAN Devices with the same Master Preference value change their role periodically due to the random portion of the Master Rank. If a NAN Device is capable of permanently maintaining a Master role (e.g., Set-top Box, TV, etc.), then it should be considered to be a NAN Infrastructure Device and it should set its Master Preference to a value greater than or equal to 128. All other NAN Devices should set its Master Preference to a value smaller than 128.

Appendix D (Normative) Bloom filter use for tracking and communicating Cluster size

A NAN Device tracks the size of the NAN Cluster to which it belongs by using a Bloom Filter. This allows a NAN Device to keep an estimate of the size of the cluster. In addition, a NAN Device may share its size tracking Bloom filter with a neighbor to provide the neighbor with an estimate of the NAN Cluster size and provide it with a starting point to track the NAN Devices in the NAN Cluster. This is especially useful if the neighbor has just joined the NAN Cluster.

It is recommended that the NAN Cluster tracking Bloom filter be 250 bytes to provide sufficient accuracy for tracking up to 2000 NAN Devices.

To track the size of a NAN Cluster with NAN Cluster ID C, devices in the NAN extract the transmitter address of frames that are received with a NAN Cluster ID C (A3 field). 4-bit position sets corresponding to hash functions in set 1 of Table 155 are computed. The bits in the 4-bit position sets are set to one (note if the bit is already set to one, its value is unchanged).

D.1 Estimating Cluster size from Bloom filter

Estimated Cluster Size = - M * ln(1 – N/M)/K.

where:

M: Size of the Tracking Bloom filter in bits (recommended 2400 = 300 bytes)

N: Number of bits in the tracking Bloom filter that are set to one (1).

K: Number of Hash Functions (4)

D.2 Aging out bits in the Bloom filter

Bits that are set in the Bloom filter should be aged out by resetting the bit to zero if no entries have set the bit for an implementation specific time out. This would prevent the Bloom Filter from over-estimating the size of the NAN Cluster by accounting for devices that are dormant for an extended time or have departed from the NAN Cluster.

Appendix E (Informative) Recommended practices for NAN security

Security may be supported by any NAN service to:

- Protect the disclosure of services being requested
- Protect the disclosure of services being revealed or announced
- Protect the service specific information shared in requests, responses, and announcements
- Limit MAC address tracking to increase mobile user privacy

These security features are capabilities built into the applications that use the NAN primitives and are not based on IEEE 802.11 MAC layer security. The following sections provide recommendations for approaches to use the NAN primitives with additional security.

E.1 NAN group security and keys

NAN optionally supports protection for group addressed data frames, multicast management frames, including Beacons by establishing the corresponding security associations (GTKSA, IGTKSA, BIGTKSA) and distributing the corresponding keys using NDP setup or Follow-up exchanges as described earlier.

A group of devices can use the NAN Publish and Subscribe functions in a secure manner by providing each member of the group with a shared secret key (NAN Group Key). Any device could be a member of multiple secure groups each with a different group key. The creation and distribution of these keys to group members is not in the scope of this specification. Typically, this distribution would be managed by a particular service that supported secure discovery with NAN. Such group enrollment and key distribution could readily be managed with a web site coordinating this membership.

E.2 Security for NAN Service Identifiers

Replacing the well-known Service ID with a pseudo random Secure Service ID can mask NAN Service IDs.

The Secure Service ID is formed by hashing the service name with the NAN Group Key. This new Service Id is then used for all Publish and Subscribe functions for the secure service discovery. Other devices in the same group will recognize the ID and process it correctly. Some applications may wish to periodically change the Secure Service Id by periodically changing the NAN Group Key for the service. This change can be synchronized by concatenating a shared NAN Master Group Key with high order octets from the NAN Cluster TSF value as the NAN Group Key. For example, using the top 4 octets of the NAN Cluster TSF as part of the NAN Group key the Secure Service ID will change every 1.3 hours.

E.3 Sharing NDIs for different types of security

Generally speaking, it is a good security practice to separate the NDIs used for traffic of different levels of security within NAN Devices. However, some NAN Devices may be resource constrained and may use the same local NDI for NDPs. They may also use the same <local, remote> NDI pair that supports both un-secure and secure data traffic. Such use is governed by device and application policy rather than mandated by the NAN specification. This is similar to other protocols such as IPsec (IETF RFC 4301), and opportunistic use of TLS (IETF RFC 7435) that share the layer endpoint among connections from different clients with differing security. NDP security setup may be rejected by a device based on such policy by returning an appropriate reason code.

Appendix F (Informative) Bloom filter verification sequences

F.1 Set 1

H(j,X,M) : M (Bloom Filter Size) = 40 bits

Table 163. Address set 1

0x00, 0x60, 0x2F, 0xBF, 0x5B, 0x92	0x00, 0x60, 0x2F, 0xCA, 0xEC, 0xBD
0x00, 0x60, 0x2F, 0x95, 0x06, 0x4B	0x00, 0x60, 0x2F, 0x76, 0x7C, 0xA5
0x00, 0x60, 0x2F, 0x3A, 0x1E, 0x03	0x00, 0x60, 0x2F, 0xFE, 0x9E, 0x6A
0x00, 0x60, 0x2F, 0x29, 0xA5, 0x5F	0x00, 0x60, 0x2F, 0xC3, 0x77, 0xE5

Table 164. Generated Bloom filter 1

J	Bloom Filter
0	0xEF, 0x8C, 0xD5, 0xE6, 0x18
1	0xAF, 0xF1, 0x7A, 0x06, 0x33
2	0xFB, 0x33, 0xF0, 0x23, 0x07
3	0x8C, 0x46, 0x8F, 0xF9, 0xFC

F.2 Set 2

H(j,X,M) : M (Bloom Filter Size) = 80 bits

Table 165. Address set 2

0x00, 0x60, 0x2F, 0x54, 0x98, 0xC8	0x00, 0x60, 0x2F, 0x8E, 0x26, 0x5E	0x00, 0x60, 0x2F, 0xD6, 0x78, 0x8F	0x00, 0x60, 0x2F, 0x59, 0x51, 0x7F
0x00, 0x60, 0x2F, 0x95, 0xE1, 0xAB	0x00, 0x60, 0x2F, 0x63, 0x90, 0xC0	0x00, 0x60, 0x2F, 0xBE, 0x8F, 0x78	0x00, 0x60, 0x2F, 0x5A, 0x47, 0x4C
0x00, 0x60, 0x2F, 0x8E, 0x69, 0xE1	0x00, 0x60, 0x2F, 0x36, 0x16, 0x4A	0x00, 0x60, 0x2F, 0x92, 0x6B, 0x03	0x00, 0x60, 0x2F, 0xBF, 0x5B, 0x92
0x00, 0x60, 0x2F, 0xFB, 0x30, 0x83	0x00, 0x60, 0x2F, 0xAB, 0x3B, 0x54	0x00, 0x60, 0x2F, 0xD7, 0xA2, 0x93	0x00, 0x60, 0x2F, 0x95, 0x06, 0x4B

Table 166. Generated Bloom filter 2

J	Bloom Filter
0	0xFB, 0x02, 0x01, 0xF7, 0x37, 0xFA, 0x55, 0x23, 0xBE, 0x3D
1	0xCF, 0x73, 0x85, 0xAE, 0xFA, 0xC0, 0xFD, 0x2C, 0x58, 0xFD
2	0x22, 0xDB, 0xEF, 0x1F, 0xCD, 0xAE, 0x3D, 0xE4, 0xD3, 0x89
3	0x7A, 0x92, 0xDD, 0x7E, 0x11, 0x27, 0x23, 0xFF, 0xFB, 0xD8

Appendix G (Informative) Open source CRC32 sample C code

The open source CRC32 sample code listed below is taken directly from [6].

```
/*-
 *  COPYRIGHT (C) 1986 Gary S. Brown.  You may use this program, or
 *  code or tables extracted from it, as desired without restriction.
 *
 *  First, the polynomial itself and its table of feedback terms.  The
 *  polynomial is
 *  X^32+X^26+X^23+X^22+X^16+X^12+X^11+X^10+X^8+X^7+X^5+X^4+X^2+X^1+X^0
 *
 *  Note that we take it "backwards" and put the highest-order term in
 *  the lowest-order bit.  The X^32 term is "implied"; the LSB is the
 *  X^31 term, etc.  The X^0 term (usually shown as "+1") results in
 *  the MSB being 1
 *
 *  Note that the usual hardware shift register implementation, which
 *  is what we're using (we're merely optimizing it by doing eight-bit
 *  chunks at a time) shifts bits into the lowest-order term.  In our
 *  implementation, that means shifting towards the right.  Why do we
 *  do it this way?  Because the calculated CRC must be transmitted in
 *  order from highest-order term to lowest-order term.  UARTs transmit
 *  characters in order from LSB to MSB.  By storing the CRC this way
 *  we hand it to the UART in the order low-byte to high-byte; the UART
 *  sends each low-bit to hight-bit; and the result is transmission bit
 *  by bit from highest- to lowest-order term without requiring any bit
 *  shuffling on our part.  Reception works similarly
 *
 *  The feedback terms table consists of 256, 32-bit entries.  Notes
 *
 *      The table can be generated at runtime if desired; code to do so
 *      is shown later.  It might not be obvious, but the feedback
 *      terms simply represent the results of eight shift/xor opera
 *      tions for all combinations of data and CRC register values
 *
 *      The values must be right-shifted by eight bits by the "updcrc
 *      logic; the shift must be unsigned (bring in zeroes).  On some
 *      hardware you could probably optimize the shift in assembler by
 *      using byte-swap instructions
 *      polynomial $edb88320
 *
 *
 * CRC32 code derived from work by Gary S. Brown.
 */

#include <sys/param.h>
#include <sys/systm.h>

static uint32_t crc32_tab[] = {
   0x00000000, 0x77073096, 0xee0e612c, 0x990951ba, 0x076dc419, 0x706af48f,
   0xe963a535, 0x9e6495a3, 0x0edb8832, 0x79dcb8a4, 0xe0d5e91e, 0x97d2d988,
   0x09b64c2b, 0x7eb17cbd, 0xe7b82d07, 0x90bf1d91, 0x1db71064, 0x6ab020f2,
   0xf3b97148, 0x84be41de, 0x1adad47d, 0x6ddde4eb, 0xf4d4b551, 0x83d385c7,
   0x136c9856, 0x646ba8c0, 0xfd62f97a, 0x8a65c9ec, 0x14015c4f, 0x63066cd9,
   0xfa0f3d63, 0x8d080df5, 0x3b6e20c8, 0x4c69105e, 0xd56041e4, 0xa2677172,
   0x3c03e4d1, 0x4b04d447, 0xd20d85fd, 0xa50ab56b, 0x35b5a8fa, 0x42b2986c,
   0xdbbbc9d6, 0xacbcf940, 0x32d86ce3, 0x45df5c75, 0xdcd60dcf, 0xabd13d59,
   0x26d930ac, 0x51de003a, 0xc8d75180, 0xbfd06116, 0x21b4f4b5, 0x56b3c423,
   0xcfba9599, 0xb8bda50f, 0x2802b89e, 0x5f058808, 0xc60cd9b2, 0xb10be924,
```

```
   0x2f6f7c87, 0x58684c11, 0xc1611dab, 0xb6662d3d, 0x76dc4190, 0x01db7106,
   0x98d220bc, 0xefd5102a, 0x71b18589, 0x06b6b51f, 0x9fbfe4a5, 0xe8b8d433,
   0x7807c9a2, 0x0f00f934, 0x9609a88e, 0xe10e9818, 0x7f6a0dbb, 0x086d3d2d,
   0x91646c97, 0xe6635c01, 0x6b6b51f4, 0x1c6c6162, 0x856530d8, 0xf262004e,
   0x6c0695ed, 0x1b01a57b, 0x8208f4c1, 0xf50fc457, 0x65b0d9c6, 0x12b7e950,
   0x8bbeb8ea, 0xfcb9887c, 0x62dd1ddf, 0x15da2d49, 0x8cd37cf3, 0xfbd44c65,
   0x4db26158, 0x3ab551ce, 0xa3bc0074, 0xd4bb30e2, 0x4adfa541, 0x3dd895d7,
   0xa4d1c46d, 0xd3d6f4fb, 0x4369e96a, 0x346ed9fc, 0xad678846, 0xda60b8d0,
   0x44042d73, 0x33031de5, 0xaa0a4c5f, 0xdd0d7cc9, 0x5005713c, 0x270241aa,
   0xbe0b1010, 0xc90c2086, 0x5768b525, 0x206f85b3, 0xb966d409, 0xce61e49f,
   0x5edef90e, 0x29d9c998, 0xb0d09822, 0xc7d7a8b4, 0x59b33d17, 0x2eb40d81,
   0xb7bd5c3b, 0xc0ba6cad, 0xedb88320, 0x9abfb3b6, 0x03b6e20c, 0x74b1d29a,
   0xead54739, 0x9dd277af, 0x04db2615, 0x73dc1683, 0xe3630b12, 0x94643b84,
   0x0d6d6a3e, 0x7a6a5aa8, 0xe40ecf0b, 0x9309ff9d, 0x0a00ae27, 0x7d079eb1,
   0xf00f9344, 0x8708a3d2, 0x1e01f268, 0x6906c2fe, 0xf762575d, 0x806567cb,
   0x196c3671, 0x6e6b06e7, 0xfed41b76, 0x89d32be0, 0x10da7a5a, 0x67dd4acc,
   0xf9b9df6f, 0x8ebeeff9, 0x17b7be43, 0x60b08ed5, 0xd6d6a3e8, 0xa1d1937e,
   0x38d8c2c4, 0x4fdff252, 0xd1bb67f1, 0xa6bc5767, 0x3fb506dd, 0x48b2364b,
   0xd80d2bda, 0xaf0a1b4c, 0x36034af6, 0x41047a60, 0xdf60efc3, 0xa867df55,
   0x316e8eef, 0x4669be79, 0xcb61b38c, 0xbc66831a, 0x256fd2a0, 0x5268e236,
   0xcc0c7795, 0xbb0b4703, 0x220216b9, 0x5505262f, 0xc5ba3bbe, 0xb2bd0b28,
   0x2bb45a92, 0x5cb36a04, 0xc2d7ffa7, 0xb5d0cf31, 0x2cd99e8b, 0x5bdeae1d,
   0x9b64c2b0, 0xec63f226, 0x756aa39c, 0x026d930a, 0x9c0906a9, 0xeb0e363f,
   0x72076785, 0x05005713, 0x95bf4a82, 0xe2b87a14, 0x7bb12bae, 0x0cb61b38,
   0x92d28e9b, 0xe5d5be0d, 0x7cdcefb7, 0x0bdbdf21, 0x86d3d2d4, 0xf1d4e242,
   0x68ddb3f8, 0x1fda836e, 0x81be16cd, 0xf6b9265b, 0x6fb077e1, 0x18b74777,
   0x88085ae6, 0xff0f6a70, 0x66063bca, 0x11010b5c, 0x8f659eff, 0xf862ae69,
   0x616bffd3, 0x166ccf45, 0xa00ae278, 0xd70dd2ee, 0x4e048354, 0x3903b3c2,
   0xa7672661, 0xd06016f7, 0x4969474d, 0x3e6e77db, 0xaed16a4a, 0xd9d65adc,
   0x40df0b66, 0x37d83bf0, 0xa9bcae53, 0xdebb9ec5, 0x47b2cf7f, 0x30b5ffe9,
   0xbdbdf21c, 0xcabac28a, 0x53b39330, 0x24b4a3a6, 0xbad03605, 0xcdd70693,
   0x54de5729, 0x23d967bf, 0xb3667a2e, 0xc4614ab8, 0x5d681b02, 0x2a6f2b94,
   0xb40bbe37, 0xc30c8ea1, 0x5a05df1b, 0x2d02ef8d
};

uint32_t
crc32(uint32_t crc, const void *buf, size_t size)
{
   const uint8_t *p;

   p = buf;
   crc = crc ^ ~0U;

   while (size--)
      crc = crc32_tab[(crc ^ *p++) & 0xFF] ^ (crc >> 8);

   return crc ^ ~0U;
}
```

For the bloom filter calculation, the code should be modified as follows:

```
uint32_t
crc32(uint32_t crc, const void *buf, size_t size)
{
   const uint8_t *p;

   p = buf;
// crc = crc ^~0U; /* Comment out complementing all bits*/

   while (size--)
```

```
      crc = crc32_tab[(crc ^ *p++) & 0xFF] ^ (crc >> 8);

   return crc; // ^ ~0U; /* Comment out complementing all bits*/
}
```

Appendix H (Informative) Matching filter examples

The following tables show some examples of Publish trigger conditions based on match operations between the matching filter field in the Subscribe message and the matching_filter_rx value given for the instance of the Publish function. In each example the value <0> represents a wildcard that will match all, and a <len,val> pair such as <1,2> is a specific value.

Matching filter field in Subscribe message	No filter	No filter	<0><0><0><0><0>	No filter	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Publish funtion	No filter	<0><0><0><0><0>	No filter	<1,1><1,2><1,3><1,4><1,5>	No filter
Meet trigger condition?	Yes	Yes	Yes	Yes	No

Matching filter field in Subscribe message	<0><0><0><0><0>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Publish funtion	<1,1><1,2><1,3><1,4><1,5>	<0><0><0><0><0>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,1><1,4><1,5>
Meet trigger condition?	Yes	Yes	Yes	No

Matching filter field in Subscribe message	<1,1><0><1,3><0><1,5>	<1,1><1,2><1,3><1,4><1,5>	<0><1,2><0><1,4>	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Publish funtion	<1,1><1,2><1,3><1,4><1,5>	<0><1,2><1,3><0><1,5>	<1,1><1,2><1,3><1,4><1,5>	<1,1><0><1,3><0>
Meet trigger condition?	Yes	Yes	Yes	No

The following tables show some examples of DiscoveryResult event declarations based on match operations between the matching filter field in the Publish message and the matching_filter_rx value given for the instance of the Subscribe function.

Matching filter field in Publish message	No filter	No filter	<0><0><0><0><0>	No filter	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Subscribe function	No filter	<0><0><0><0><0>	No filter	<1,1><1,2><1,3><1,4><1,5>	No filter
Declare *DiscoveryResult* event?	Yes	Yes	Yes	No	Yes

Matching filter field in Publish message	<0><0><0><0><0>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Subscribe function	<1,1><1,2><1,3><1,4><1,5>	<0><0><0><0><0>	<1,1><1,2><1,3><1,4><1,5>	<1,1><1,2><1,1><1,4><1,5>
Declare *DiscoveryResult* event?	Yes	Yes	Yes	No

Matching filter field in Publish message	<1,1><0><1,3><0><1,5>	<1,1><1,2><1,3><1,4><1,5>	<0><1,2><0><1,4>	<1,1><1,2><1,3><1,4><1,5>
matching_filter_rx for Subscribe function	<1,1><1,2><1,3><1,4><1,5>	<0><1,2><1,3><0><1,5>	<1,1><1,2><1,3><1,4><1,5>	<1,1><0><1,3><0>
Declare *DiscoveryResult* event?	Yes	Yes	No	Yes

Appendix I (Normative) GAS frames for NAN Further Service Discovery

I.1 NAN Further Service Discovery Request ANQP element

The values of all reserved fields shall be zero on transmission and ignored upon reception. In addition, little endian encoding is used for multi-octet fields and subfields. The Further Service Discovery Request is distinguished from the Response as the GAS header includes a bit identifying whether the message is a request or response.

The NAN Further Service Request Discovery ANQP elements provide additional means to discover service attributes and is sent during the NAN Further Service Discovery period as described in section 4.3. This element is formatted as defined by the ANQP vendor-specific list element, see section 9.4.5.8 in [1], shown in Figure 75. The OI Subtype and subsequent fields comprise the Vendor Specific Content as shown in Figure 9-602 [1].

Octets:	2	2	3	1	1	variable
	Info ID	**Length**	**Vendor OI**	**OI Subtype**	**Service Update Indicator**	**NAN Further Service Discovery Request Tuples**

Figure 75. Further NAN Service Discovery Request ANQP Element format

Where:

The Info ID field is a 2-octet subfield whose value is the value for the vendor-specific ANQP element (value 56797, see Table 9-271 in [1]).

The Length field is a 2-octet field whose value is set to 4 plus the length of the NAN Further Service Discovery Request Tuples.

The Vendor OI is a 3-octet field and is defined in section 9.4.5.8 in [1]. The Vendor OI field is set to the value used by Wi-Fi Alliance (value 0x506F9A).

The OI Subtype is a 1-octet field set to the value 0x13.

The Service Update Indicator is a counter that is incremented when a change has occurred in the service information of the NAN Device sending this Query Request frame. In case the Service Update Indicator is not used, this field is set to zero.

The NAN Further Service Discovery Request Tuples field is a variable length field containing one or more NAN Further Service Discovery Request Tuple fields as defined in Figure 76.

Octets:	2	1	1	variable
	Length	**NAN Service Protocol Type**	**NAN Publish ID**	**Query Data**

Figure 76. Further NAN Service Discovery Request Tuple field

The Length field is a 2-octet sub-field whose value is set to two plus the length of the Query Data sub-field.

The NAN Service Protocol Type field is a 1-octet sub-field whose values are defined in Figure 75.

The NAN Publish ID is a 1-octet sub-field set to the corresponding Publish ID in the NAN Publish message.

The Query Data sub-field value is dependent on the requested NAN Service Protocol Type. The Query Data field shall include the service information pertaining to the requested NAN service protocol type.

The Length, NAN Service Protocol Type, NAN Publish ID and Query Data fields form a TLV structure. There may be one or more such TLV structures in the NAN Further Service Discovery Request Tuples field of the ANQP Query Request frame.

Table 167. NAN Service Protocol Type definition

Element Name	Subtype Value	Description
Reserved	0-254	
Vendor Specific	255	

I.2 NAN Further Service Discovery Response ANQP Element

The values of all reserved fields shall be zero on transmission and ignored upon reception. In addition, little endian encoding is used for multi-octet fields and subfields. The Further Service Discovery Response is distinguished from the request as the GAS header includes a bit identifying whether the message is a request or response.

The Further NAN Service Request Discovery Response ANQP element provides additional means to discover service attributes and is sent during the NAN Further Service Discovery period in response to a NAN Further Service Discovery Request ANQP element. This element is formatted as defined by the ANQP vendor-specific list element, see section 9.4.5.8 in [1], shown in Figure 77. The OI Subtype and subsequent fields comprise the Vendor Specific Content as shown in Figure 9-602 [1].

Octets:	2	2	3	1	1	variable
	Info ID	**Length**	**Vendor OI**	**OI Subtype**	**Service Update Indicator**	**NAN Further Service Discovery Response Tuples**

Figure 77. Further NAN Service Discovery Response ANQP Element format

Where:

The Info ID field is a 2-octet sub-field whose value is the value for the vendor-specific ANQP-element (value 56797, see Table 9-271 in [1]).

The Length field is a 2-octet sub-field whose value is set to 5 plus the length of the NAN Further Service Discovery Response Tuples field.

The Vendor OI is a 3-octet sub-field and is defined in section 9.4.5.8 in [1]. The Vendor OI field is set to the value used by Wi-Fi Alliance (value 0x 506F9A).

The OI Subtype is a 1-octet field set to the value 0x13.

The Service Update Indicator is a counter that is incremented when a change has occurred in the service information of the NAN Device sending this Query Response frame. In case the Service Update Indicator is not used this field is set to zero.

The NAN Further Service Discovery Response Tuples field is a variable length field containing one or more NAN Further Service Discovery Response Tuple fields as defined in Figure 78.

Octets:	2	1	1	1	variable
	Length	NAN Service Protocol Type	NAN Publish ID	NAN Further Service Discovery Status Code	Response Data

Figure 78. Further NAN Service Discovery Response Tuple field

Where:

The Length field is a 2-octet subfield whose value is set to 3 plus the length of the Response Data subfield.

The NAN Service Protocol Type field is a 1-octet field whose values are defined in Table 167.

The NAN Publish ID is a 1-octet field set to the corresponding Publish ID in the NAN Publish message.

The NAN Further Service Discovery Status Code is a 1-octet field set to the corresponding value in Figure 77.

The Response Data field value is dependent on the NAN Service Protocol Type. The Response Data field shall include the service information pertaining to the NAN service protocol type.

The Length, NAN Service Protocol Type, NAN Publish ID, NAN Further Service Discovery Status Code, and Response Data fields form a TLV structure. There may be one or more such TLV structures in the NAN Further Service Discovery Response Tuples field of the ANQP Query Response frame.

Table 168. NAN Further Service Discovery Response status codes

Value	Meaning
0	Success
1	Service not available
2	Publisher response not available
3	Unknown failure
4	Publisher response too large
4-255	Reserved

Appendix J (Normative) Internet protocol version 6 (IPv6)

NAN Devices can use IPv6 link local addresses for IP based data communications. Figure 79 shows the NDP setup handshakes that enable both the NDP Initiator and the NDP Responder to obtain each other's NDIs, and generate each other's IPv6 link local addresses accordingly.

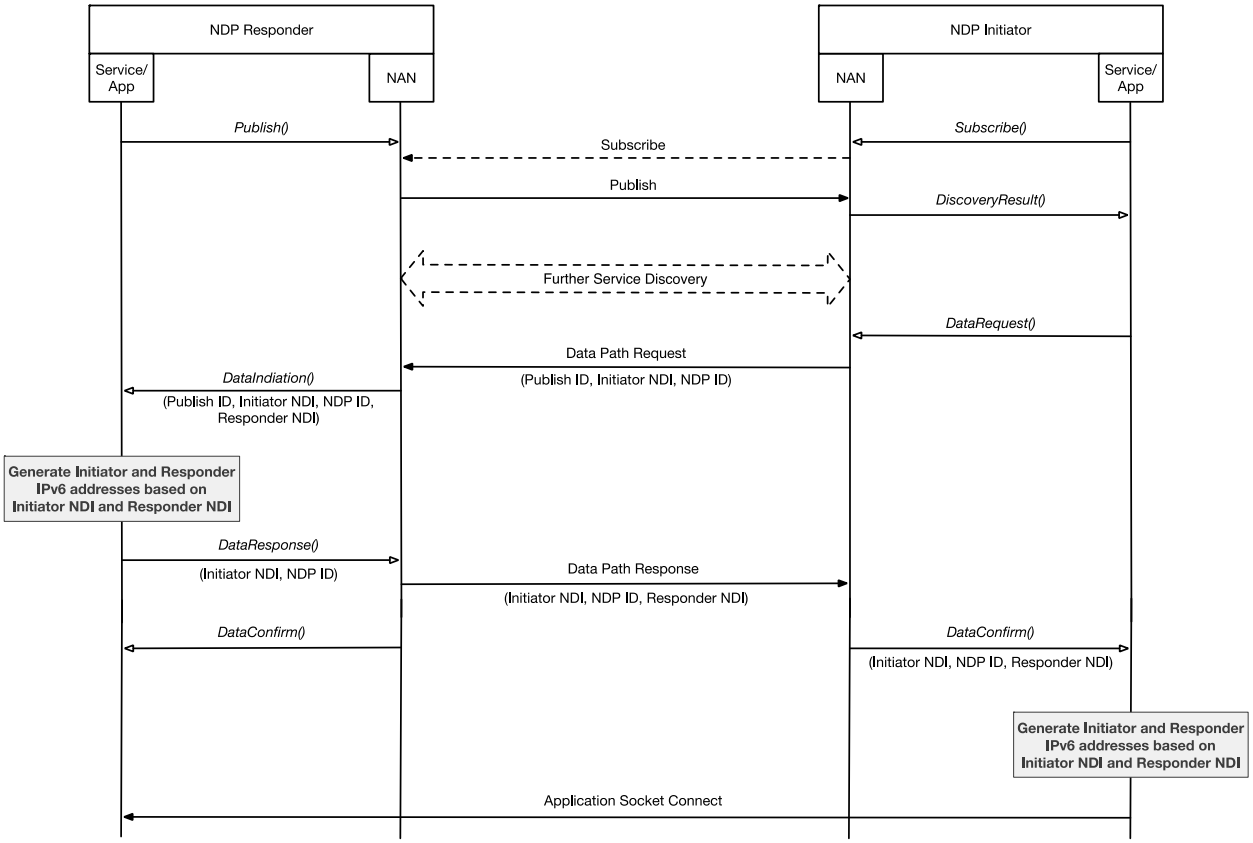


Figure 79. NDP setup for IPv6 link local address based unicast data communication

An IPv6 link local address is formed by combining the well-known link-local prefix FE80::0 with a 64-bit interface identifier.

Appendix A of [7] defines a mechanism for generating a 64-bit IEEE EUI-64 interface identifier from a 48-bit MAC Address, e.g. the NDI, as illustrated in Figure 80.

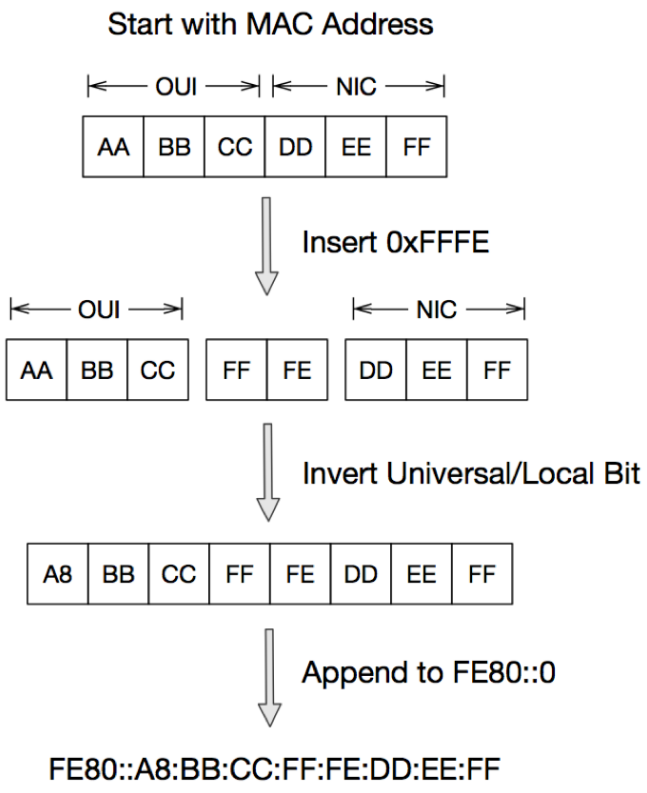


Figure 80. MAC address to IPv6 link local address conversion

Figure 81 gives an example quoted from http://ben.akrin.com/?p=1347, which also provides an online converter.

1. take the mac address: for example 52:74:f2:b1:a8:7f
2. throw ff:fe in the middle: 52:74:f2:ff:fe:b1:a8:7f
3. reformat to IPv6 notation 5274:f2ff:feb1:a87f
4. convert the first octet from hexadecimal to binary: 52 -> 01010010
5. invert the bit at index 6 (counting from 0): 01010010 -> 01010000
6. convert octet back to hexadecimal: 01010000 -> 50
7. replace first octet with newly calculated one: 5074:f2ff:feb1:a87f
8. prepend the link-local prefix: fe80::5074:f2ff:feb1:a87f
9. done!

Figure 81. MAC address to IPv6 link local address conversion example

Appendix K (Informative) Example NDL Schedule Proposals

Selecting a NDL Schedule Proposal is implementation specific. This section documents a few examples of the NDL Schedule Proposal.

Examples 1 - 4 show when a NAN Device operates on 2.4 GHz band only.

Example 1: The 2.4 GHz NAN Discovery Channel, i.e., channel 6, is used as the sole operating channel. The NDC CRB is immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots.

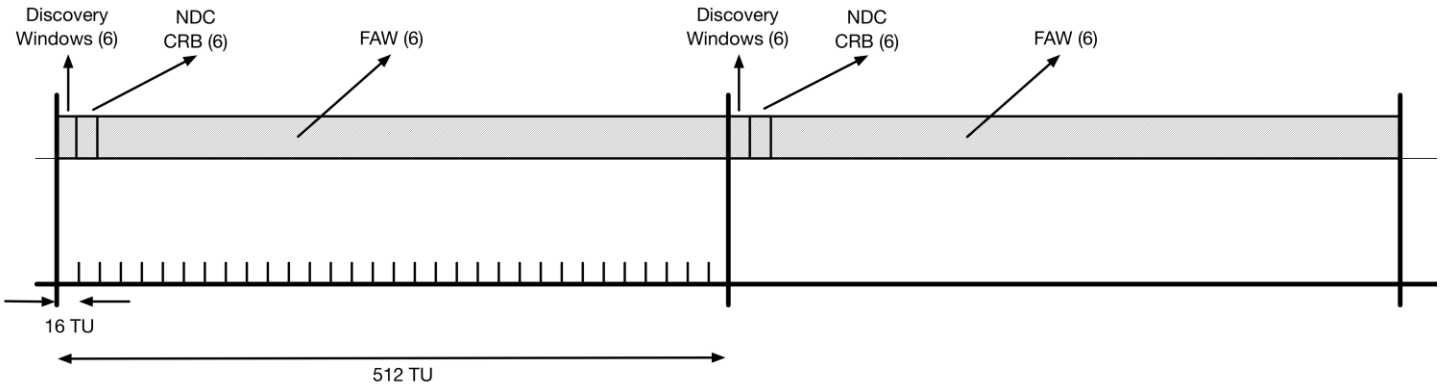


Figure 82. NDL Schedule Proposal Example 1

Example 2: An alternative channel X, other than channel 6, is used as the major operating channel. The NDC CRB is still on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. A NAN Device can propose this schedule when it detects channel 6 is too congested, or to avoid burdening channel 6.

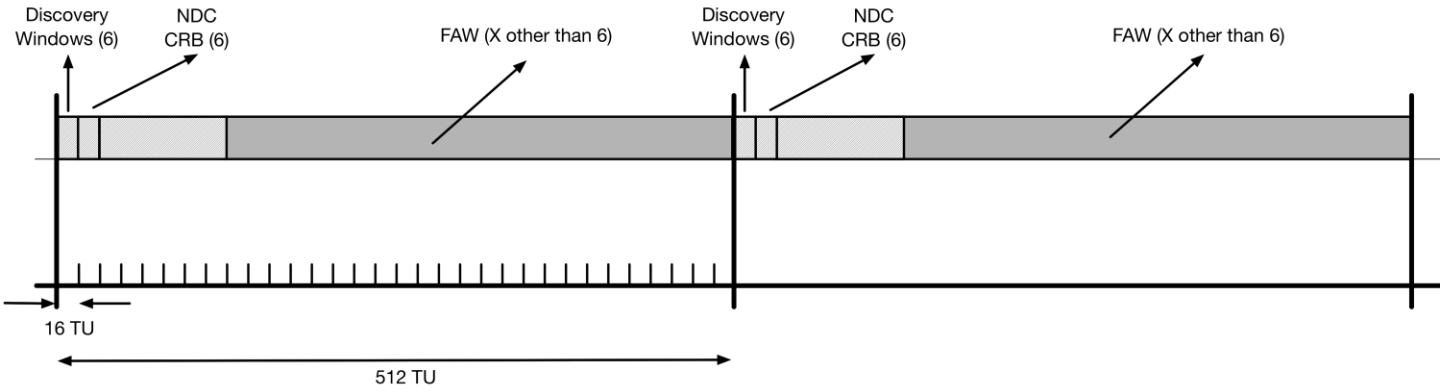


Figure 83. NDL Schedule Proposal Example 2

Example 3: The 2.4 GHz NAN Discovery Channel, i.e., channel 6, is used as the major operating channel. The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel Y, which, for example, can accommodate concurrent non-NAN operations.

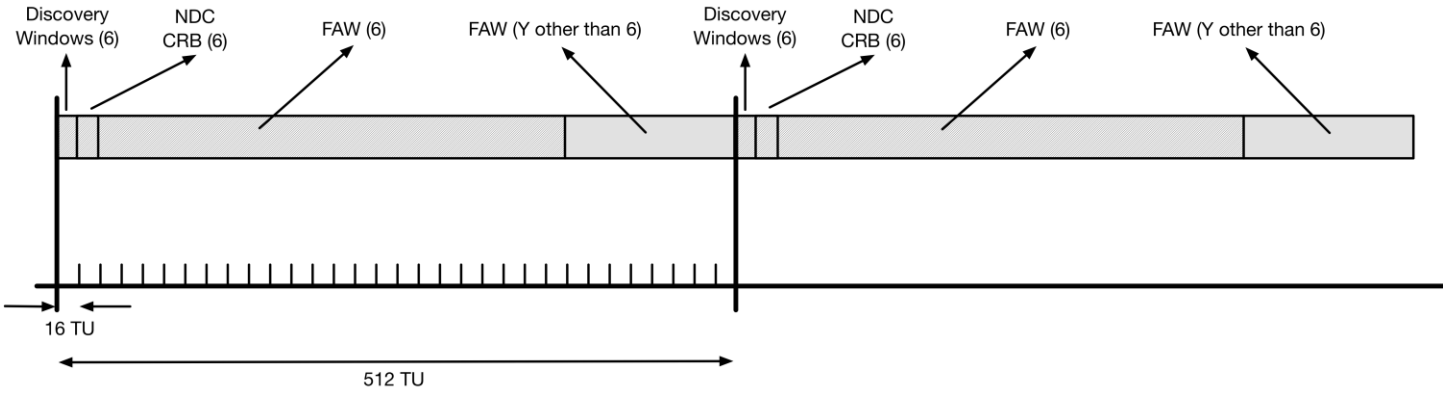


Figure 84. NDL Schedule Proposal Example 3

Example 4: An alternative channel X is used as the major operating channel. The NDC CRB is still on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel Y, which can accommodate concurrent non-NAN operations.

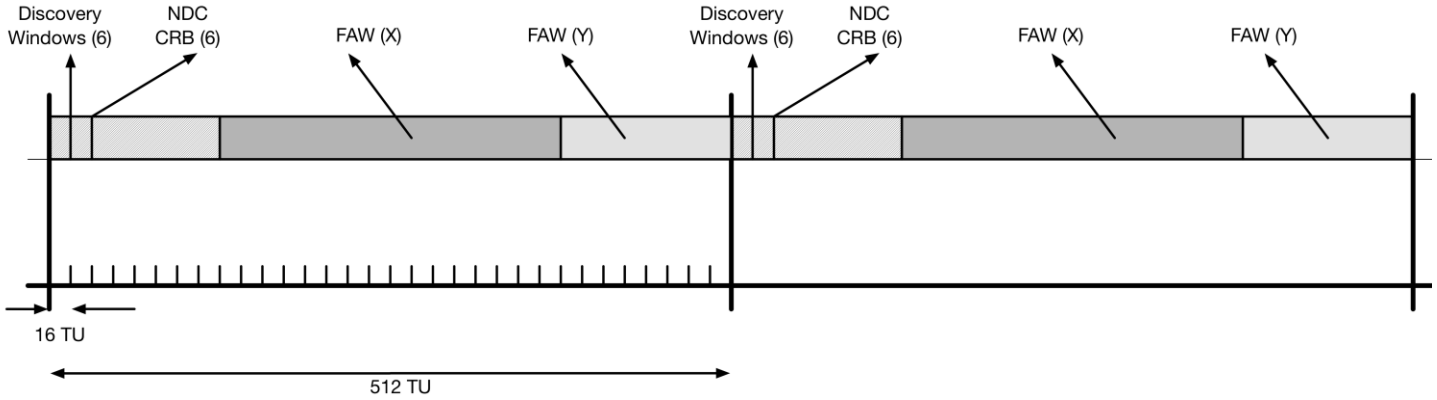


Figure 85. NDL Schedule Proposal Example 4

Examples 5 -11 show when a NAN Device operates on both 2.4 GHz and 5 GHz bands, but schedules most of the operations on 5 GHz band.

Example 5: The 5 GHz NAN Discovery Channel, i.e., channel 149 or channel 44, is used as the major operating channel. The NDC CRB is immediately subsequent to each 5 GHz Discovery Window, and contains one or more NAN Slots.

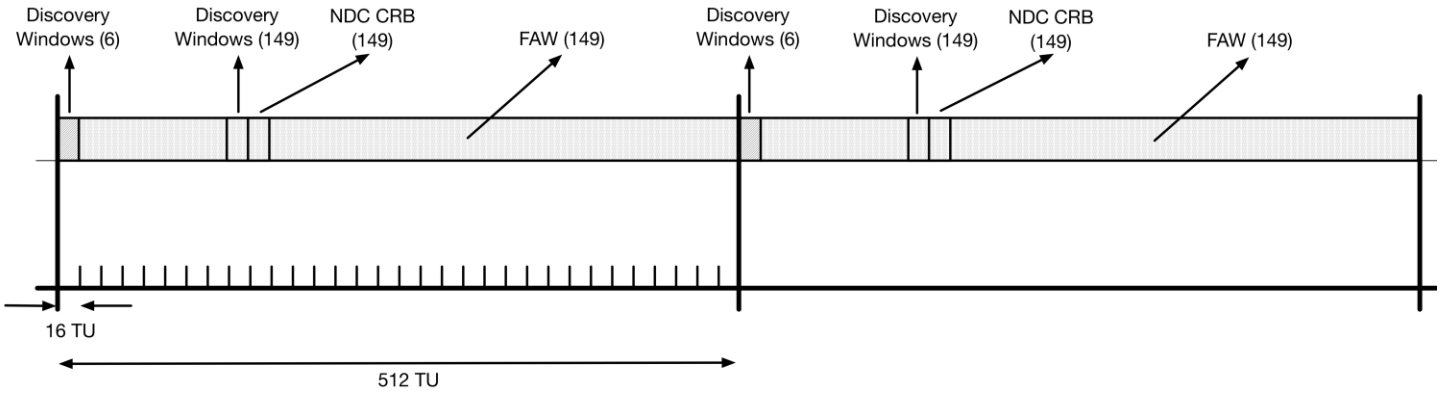


Figure 86. NDL Schedule Proposal Example 5

Example 6: An alternative channel A, other than channel 149 or 44, is used as the major operating channel. The NDC CRB is still on channel 149 or 44, immediately subsequent to each 5 GHz Discovery Window, and contains one or more

NAN Slots. A NAN Device can propose this schedule when it detects channel 149 or 44 is too congested, or to avoid burdening the NAN discovery channels.

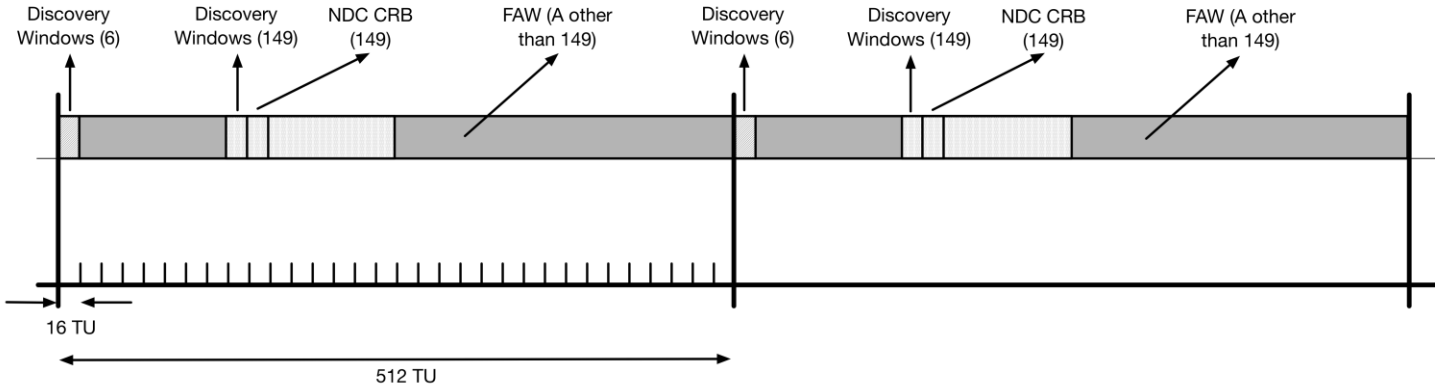


Figure 87. NDL Schedule Proposal Example 6

Example 7: The 5 GHz NAN Discovery Channel, i.e., channel 149 or 44, is used as the major operating channel. The NDC CRB is on channel 149 or 44, immediately subsequent to each 5 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations.

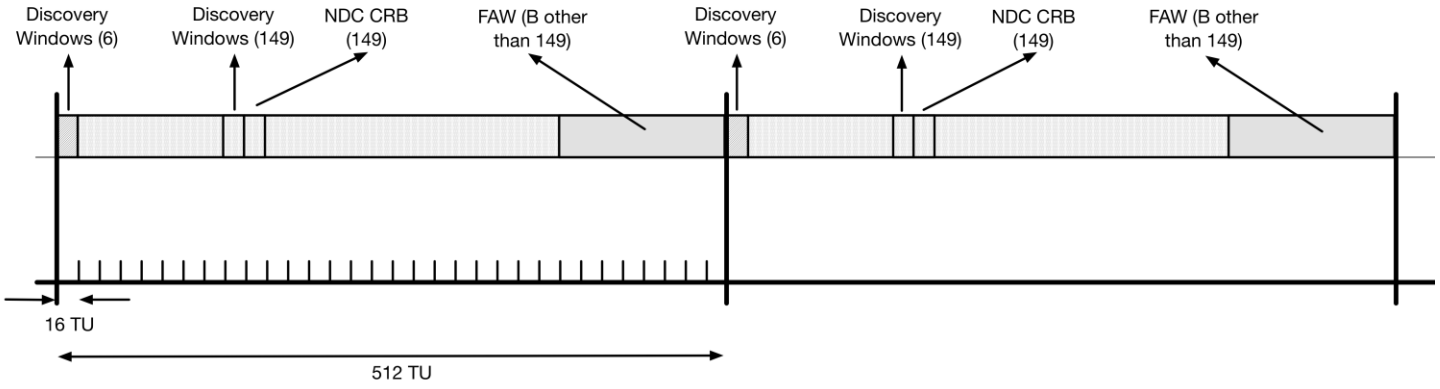


Figure 88. NDL Schedule Proposal Example 7

Example 8 and 9: The 5 GHz NAN Discovery Channel, i.e., channel 149 or 44, is used as the major operating channel. The NDC CRB is on channel 149 or 44, immediately subsequent to each 5 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations, while some other portion of the proposed schedule is on a different alternative channel C, which, for example, can accommodate the peer device's concurrent non-NAN operations.

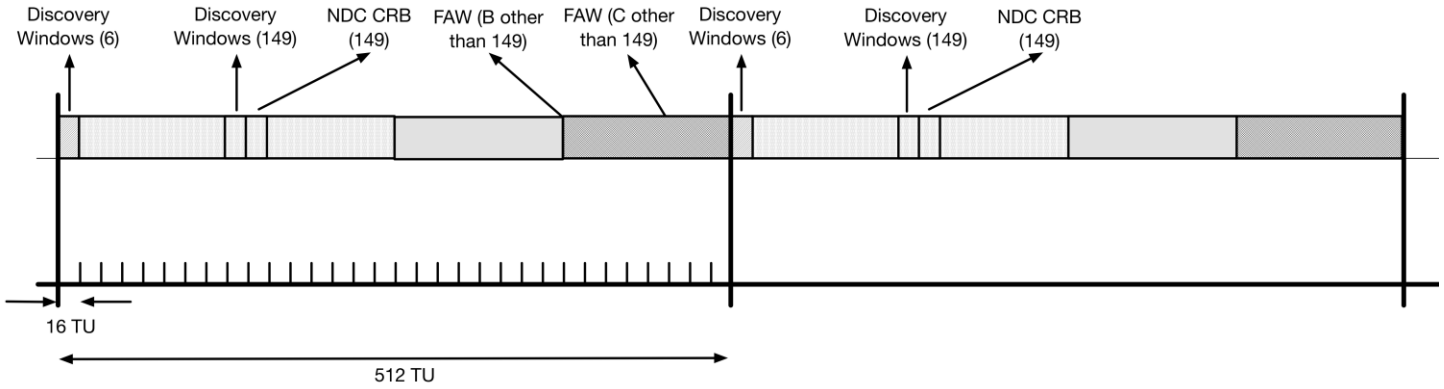


Figure 89. NDL Schedule Proposal Example 8

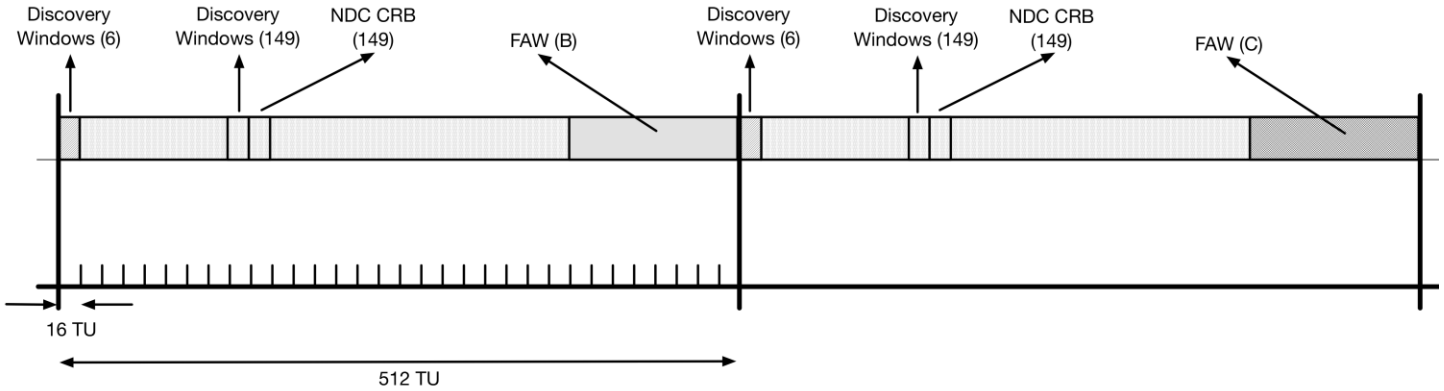


Figure 90. NDL Schedule Proposal Example 9

Example 10: An alternative channel A is used as the major operating channel. The NDC CRB is still on channel 149 or 44, immediately subsequent to each 5 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations.

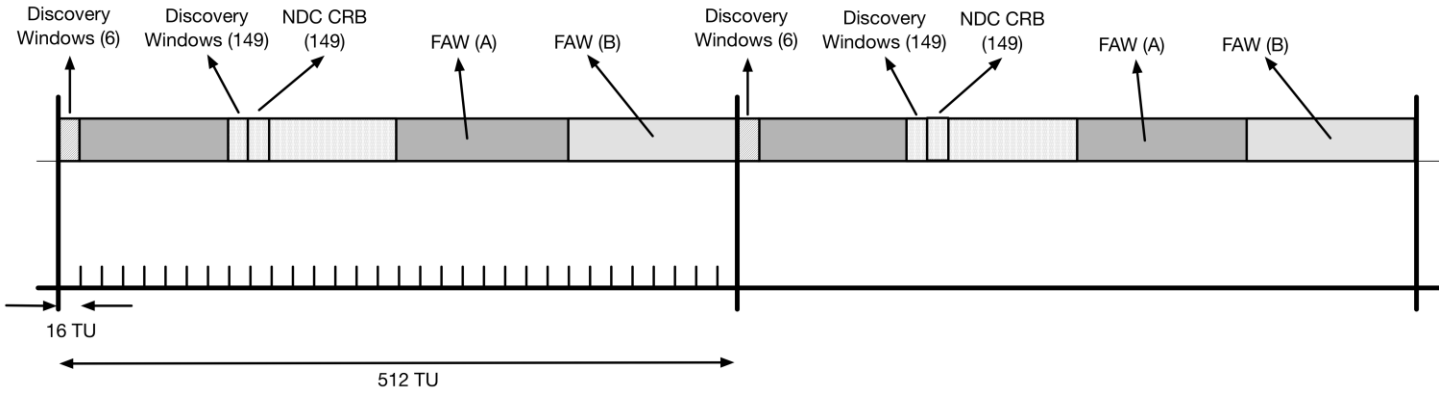


Figure 91. NDL Schedule Proposal Example 10

Example 11: An alternative channel A is used as the major operating channel. The NDC CRB is still on channel 149 or 44, immediately subsequent to each 5 GHz Discovery Window, and contains one or more NAN Slots. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations, while some other portion of the proposed schedule is on a different alternative channel C, which can accommodate the peer device's concurrent non-NAN operations.

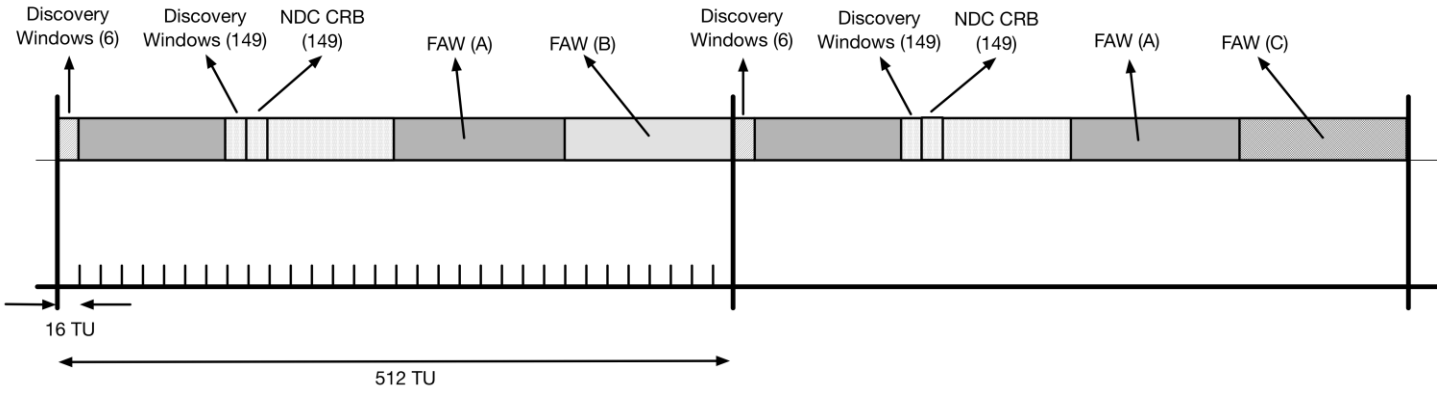


Figure 92. NDL Schedule Proposal Example 11

Examples 12-16 show when a NAN Device operates on both 2.4 GHz and 5 GHz bands, and schedules sufficient resources on both bands to accommodate 2.4 GHz/5 GHz peer NAN Devices, as well as 2.4 GHz only peer NAN Devices.

Example 12: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 is also used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5 GHz Discovery Window. The 5 GHz NAN Discovery Channel, i.e. channel 149 or channel 44, is used as the major operating channel between each 5 GHz Discovery Window and subsequent 2.4 GHz Discovery Window.

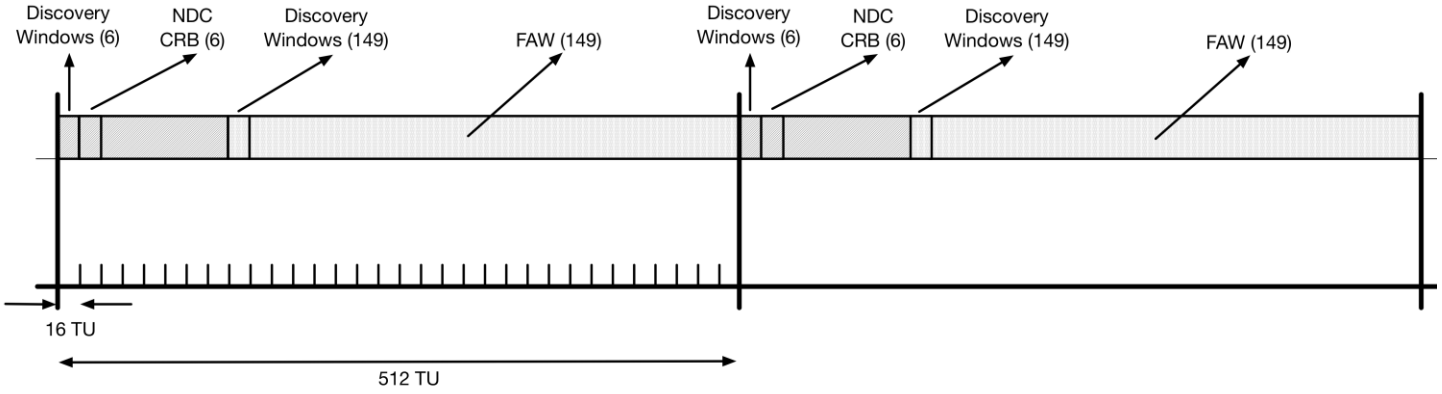


Figure 93. NDL Schedule Proposal Example 12

Example 13: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 or an alternative 2.4 GHz channel is used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5 GHz Discovery Window. An alternative channel A is used as the major operating channel between each 5GHz Discovery Window and next 2.4 GHz Discovery Window.

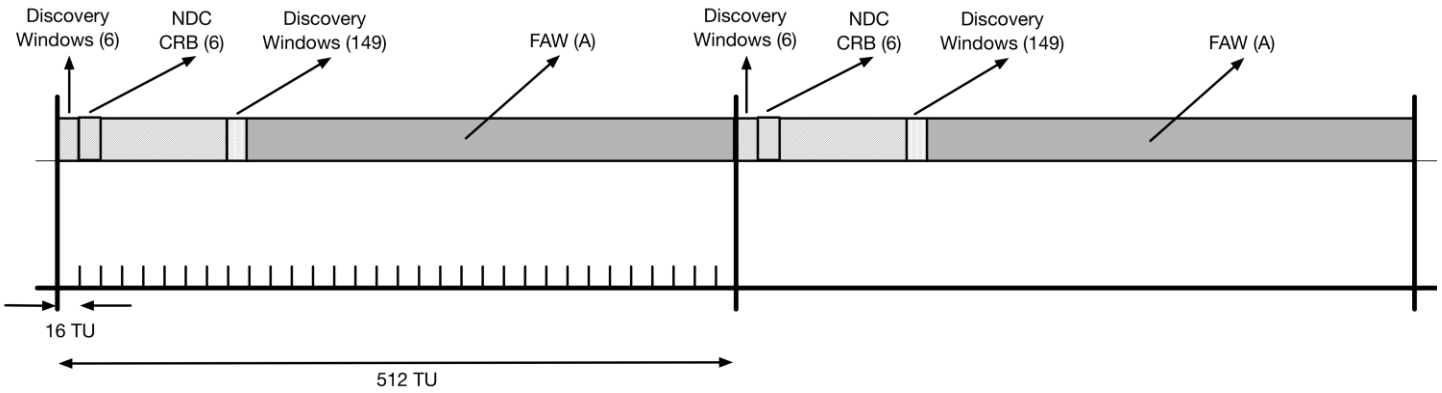


Figure 94. NDL Schedule Proposal Example 13

Example 14: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 is also used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5 GHz Discovery Window. The 5 GHz NAN Discovery Channel, i.e., channel 149 or channel 44, is used as the major operating channel between each 5 GHz Discovery Window and subsequent 2.4 GHz Discovery Window. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations.

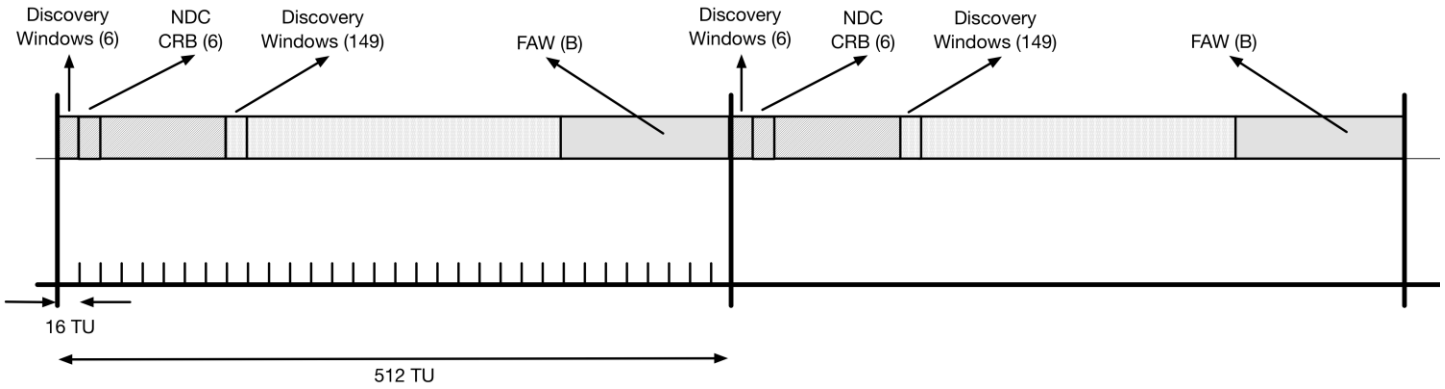


Figure 95. NDL Schedule Proposal Example 14

Example 15: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 is also used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5GHz Discovery Window. The 5 GHz NAN Discovery Channel, i.e., channel 149 or channel 44, is used as the major operating channel between each 5 GHz Discovery Window and subsequent 2.4 GHz Discovery Window. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations, while some other portion of the proposed schedule is on a different alternative channel C, which, for example, can accommodate peer device's concurrent non-NAN operations.

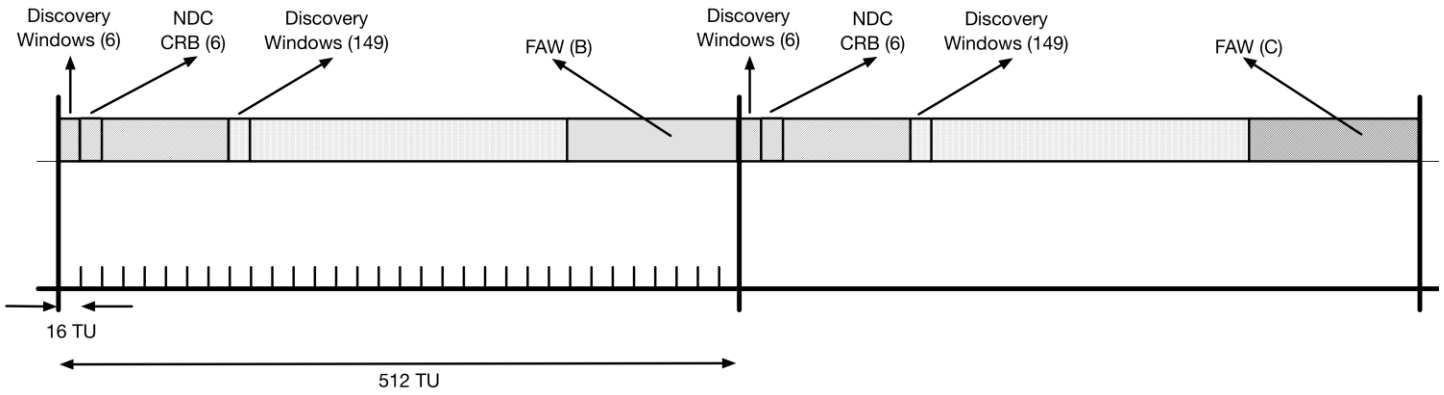


Figure 96. NDL Schedule Proposal Example 15

Example 16: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 or an alternative 2.4 GHz channel is used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5GHz Discovery Window. An alternative channel A is used as the major operating channel between each 5 GHz Discovery Window and next 2.4 GHz Discovery Window. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations.

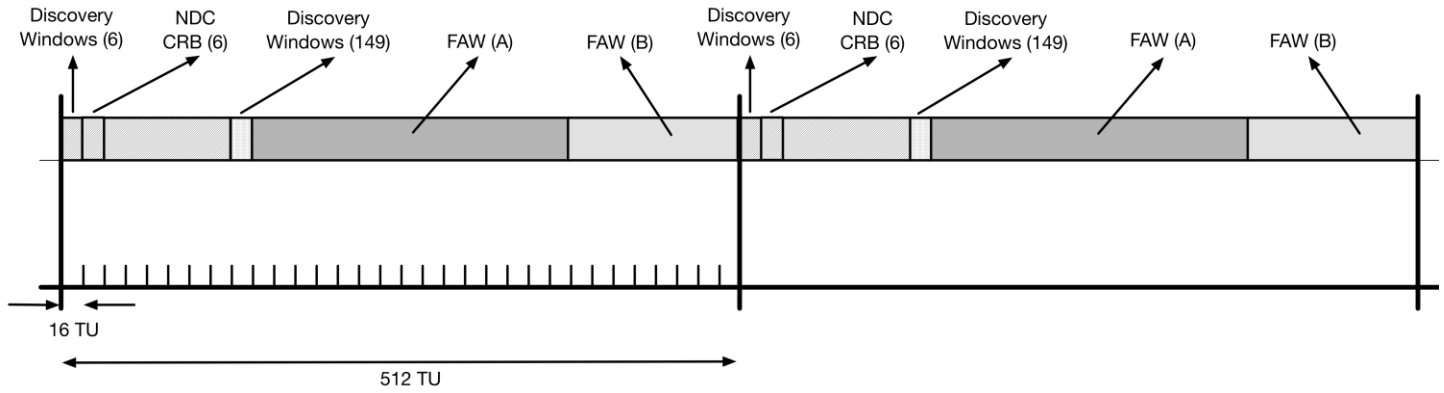


Figure 97. NDL Schedule Proposal Example 16

Example 17: The NDC CRB is on channel 6, immediately subsequent to each 2.4 GHz Discovery Window, and contains one or more NAN Slots. Channel 6 or an alternative 2.4 GHz channel is used as the major operating channel for the remaining NAN Slots (if any) between the 2.4 GHz Discovery Window and subsequent 5 GHz Discovery Window. An alternative channel A is used as the major operating channel between each 5 GHz Discovery Window and next 2.4 GHz Discovery Window. Some portion of the proposed schedule is on an alternative channel B, which can accommodate concurrent non-NAN operations, while some other portion of the proposed schedule is on a different alternative channel C, which can accommodate the peer device's concurrent non-NAN operations.

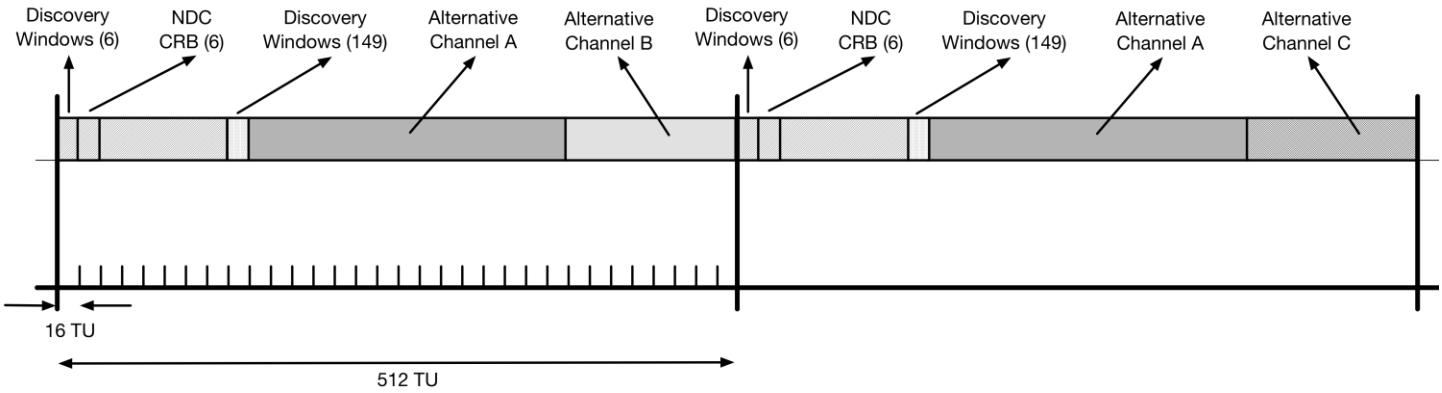


Figure 98. NDL Schedule Proposal Example 17

Appendix L (Informative) Example messages M1-M4 and test vectors

L.1 M1 message fields

Descriptor Type = 2

Key Information:

- Key Descriptor Version = 0, Key Type = 1 (Pairwise), Install = 1, Key Ack = 1, Key MIC = 0, Secure = 0, Error = 0, Request = 0, Encrypted Key Data = 0, SMK Message = 0
- Key Length = 0
- Key Replay Counter = n
- Key Nonce = INonce
- EAPOL-Key IV = 0
- Key RSC = 0
- Key MIC = 0
- Key Data Length = 0
- Key Data = None

L.2 M2 message fields

Descriptor Type = 2

Key Information:

- Key Descriptor Version = 3, Key Type = 1 (Pairwise), Install = 0, Key Ack = 0, Key MIC = 1,
- Secure = 0, Error = 0, Request = 0, Encrypted Key Data = 0, SMK Message = 0
- Key Length = 0
- Key Replay Counter = n
- Key Nonce = RNonce
- EAPOL-Key IV = 0
- Key RSC = 0
- Key MIC = MIC(ND-KCK, Body of M2 (with Key MIC field initialized to 0s) that includes additional NAN attributes used for NDP setup)
- Key Data Length = 0 if no Key Data included. Otherwise, it is the length of Key Data
- Key Data = None if not required.

L.3 M3 message fields

Descriptor Type = 2

Key Information:

- Key Descriptor Version = 3, Key Type = 1 (Pairwise), Install = 1, Key Ack = 1, Key MIC = 1,
- Secure = 1, Error = 0, Request = 0, Encrypted Key Data = 1, SMK Message = 0
- Key Length = 0
- Key Replay Counter = n+1
- Key Nonce = INonce
- EAPOL-Key IV = 0
- Key RSC = 0
- Key MIC = MIC(ND-KCK, Authentication Token || Body of M3)
- Key Data Length = 0 if no Key Data included. Otherwise, it is the length of Key Data
- Key Data = None if not required

L.4 M4 message fields

Descriptor Type = 2

Key Information:

- Key Descriptor Version = 3, Key Type = 1 (Pairwise), Install = 0, Key Ack = 0, Key MIC = 1,
- Secure = 1, Error = 0, Request = 0, Encrypted Key Data = 0, SMK Message = 0
- Key Length = 0
- Key Replay Counter = n+1
- Key Nonce = 0
- EAPOL-Key IV = 0
- Key RSC = 0
- Key MIC = MIC(ND-KCK, Body of M4(with Key MIC field initialized to 0s))
- Key Data Length = 0
- Key Data = None if not required

Appendix M (Informative) Mapping pass-phrase to ND-PMK for NCS-SK cipher suites

NCS-SK cipher suites require a 32 octet ND-PMK. However, when a stronger method of ND-PMK derivation is unavailable, practical considerations may dictate the use of a shorter pass phrase to derive the ND-PMK. Notwithstanding the limitation that keys derived from pass phrases, especially when they are short, make attacks against NCS-SK easier, this appendix provides a recommendation for mapping a pass phrase to ND-PMK when used with NCS-SK cipher suites for interoperability.

The recommended pass-phrase mapping is PBKDF2 as defined in [8] section 5.2.

> ND-PMK = PBKDF2(<pass phrase>, <Salt Version>||<Cipher Suite ID>||<Service ID>||<Publisher NMI>, 4096, 32)

Where <Salt Version> is set to zero, || is the concatenation operator, and other parameters have their usual semantics. The hash function used shall be the KDF specified for the cipher suite in section 7.1.2.

The mapping function is the same as in section J.4.1 of [1] except the SSID is replaced with the NAN specific information and the hash function used is the cipher suite as specified above rather than HMAC-SHA-1.

M.1 Example test vectors for pass-phrase to ND-PMK conversion

All data specified below is in 'hex' format unless other specified in the parenthesis.

Test Vector 1

```
Passphrase (ascii): NAN
Cipher ID: 01
Service Id: 2b9c450f6671
NMI: 02904c12d001
Salt Version: 00
Salt: 00012b9c450f667102904c12d001
PMK: ee3585063056d164d15454ad39010d4e2640b0d82fb24a2d6899862d273c68bf
```

Test Vector 2

```
Passphrase (string): NAN2
Cipher ID: 01
Service ID: 2b9c450f6671
NMI: 02904c12d001
Salt Version: 00
Salt: 00012b9c450f667102904c12d001
PMK: 87534fa774b1732db04266c42c5d08d09e5863d1da11ce2576a8f155fe26cd2a
```

Test Vector 3

```
Passphrase (string): NAN-Testvector-Phrase
Cipher ID: 01
Service name (string): NAN-Secure-Service-A
Service Id: 2b9c450f6671
NMI: 02904c12d001
Salt Version: 00
Salt: 00012b9c450f667102904c12d001
PMK: 4dc86ccda804f4e2e139fca5ddd21ba5c0b1b6ed31ffd7005e2d56f1e7bf5187
```

Appendix N (Informative) BLE TDS example test vectors

This appendix provides test vectors for the BLE TDS frames with the frame format defined in section 11.1. The TDS Flags field definition is quoted for reference in Table 169.

Table 169. TDS Flag field definition

Bits	Subfield Name	Description
0-1	Frame Role	0b00: Not specified 0b01: Seeker Only 0b10: Provider Only 0b11: Both Seeker and Provider
2	Transport Data Incomplete	0: False 1: True (more data in GATT database)
3-4	Transport State	0b00: Off 0b01: On and Available 0b10: On and Temporarily Unavailable 0b11: Reserved for future use
5-7	Reserved	Reserved for future use

N.1 Seeker Start (M1)

N.1.1 Seeker Start (M1) example test vector 1

Table 170 provides an example of a Seeker Start (M1) test vector.

Table 170. Seeker Start (M1) example test vector 1

Fields	Value	Notes
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x40, 0x11, 0x00, 0x04, 0x00, 0x08, 0x00, 0x40, 0x04, 0x04	Bloom Filter elements: s:_ipp._tcp%nan s:_ipp._tcp%p2p
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x01, 0x0B, 0x00, 0x40, 0x11, 0x00, 0x04, 0x00, 0x08, 0x00, 0x40, 0x04, 0x04};	

N.1.2 Seeker Start (M1) example test vector 2

Table 171 provides an example of a Seeker Start (M1) test vector.

Table 171. Seeker Start (M1) example test vector 2

Fields	Value	Note
AD length	0x19	25 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x15	21 bytes
Header	0x01	Bloom Filter Length: 20 bytes Channel Information: Not Present
Bloom Filter	0x40, 0x00, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00, 0x21, 0x40, 0x00, 0x01, 0x00, 0x20, 0x08, 0x00, 0x00, 0x00, 0x00	Bloom Filter elements: s:_ipp._tcp%nan s:_ipp._tcp%p2p
Test vector (starting from the AD Type Code)	uint8_t m1_len20[] = {0x26, 0x02, 0x01, 0x15, 0x01, 0x40, 0x00, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00, 0x21, 0x40, 0x00, 0x01, 0x00, 0x20, 0x08, 0x00, 0x00, 0x00, 0x00};	

N.1.3 Seeker Start (M1) test vector 3

Table 172 provides an example of a Seeker Start (M1) test vector.

Table 172. Seeker Start (M1) example test vector 3

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x11, 0x00, 0x00, 0x00, 0x08, 0x00, 0x00, 0x00, 0x04	Bloom Filter elements: s:_ipp._tcp%nan
Test Vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x01, 0x0B, 0x00, 0x00, 0x11, 0x00, 0x00, 0x00, 0x08, 0x00, 0x00, 0x00, 0x04};	

N.2 Provider responds to Seeker (M2)

N.2.1 Provider responds to Seeker (M2) example test vector 1

Table 173 provides an example of a Provider Responds to Seeker (M2) test vector.

Table 173. Provider Responds to Seeker (M2) example test vector 1

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field

Fields	Value	Note
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x02	Frame role: Provider Only Transport State: Off
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x40, 0x00, 0x00, 0x80, 0x01, 0x04, 0x00, 0x00, 0x00	Bloom Filter elements: p:_ipp._tcp%nan
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x02, 0x0B, 0x00, 0x00, 0x40, 0x00, 0x00, 0x80, 0x01, 0x04, 0x00, 0x00, 0x00};	

N.2.2 Provider Responds to Seeker (M2) example test vector 2

Table 174 provides an example of a Provider Responds to Seeker (M2) test vector.

Table 174. Provider Responds to Seeker (M2) example test vector 2

Fields	Value	Note
AD length	0x19	25 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x02	Frame role: Provider Only Transport State: Off
Transport Data Length	0x15	21 bytes
Header	0x01	Bloom Filter Length: 20 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x04, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x80, 0x00, 0x00	Bloom Filter elements: p:_ipp._tcp%nan
Test Vector (starting from the AD Type Code)	uint8_t m1_len20[] = {0x26, 0x02, 0x02, 0x15, 0x01, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x04, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x80, 0x00, 0x00};	

N.3 Seeker Connect (M3)

N.3.1 Seeker Connect (M3) example test vector 1

Table 175 provides an example of a Seeker Connect (M3) test vector.

Table 175. Seeker Connect (M3) example test vector 1

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x09	Frame role: Seeker Only

Fields	Value	Note
		Transport State: ON Note that the Frame Role may also be set as “Not Specified”, in which case, TDS Flags = 0x08
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x02, 0x02, 0x40	Bloom Filter elements: a;bta=11:22:33:aa:bb:cc:_ipp._tcp%nan
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x09, 0x0B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x02, 0x02, 0x40};	

N.3.2 Seeker Connect (M3) example test vector 2

Table 176 provides an example of a Seeker Connect (M3) test vector.

Table 176. Seeker Connect (M3) example test vector 2

Fields	Value	Note
AD length	0x19	25 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x09	Frame role: Seeker Only Transport State: ON Note that the Frame Role may also be set as “Not Specified”, in which case, TDS Flags = 0x08
Transport Data Length	0x15	21 bytes
Header	0x01	Bloom Filter Length: 20 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x00, 0x00, 0x10, 0x00, 0x00, 0x00, 0x02, 0x00, 0x00, 0x00, 0x00, 0x10, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00	Bloom Filter elements: a;bta=11:22:33:aa:bb:cc:_ipp._tcp%nan
Test vector (starting from the AD Type Code)	uint8_t m1_len20[] = {0x26, 0x02, 0x09, 0x15, 0x01, 0x00, 0x00, 0x00, 0x00, 0x10, 0x00, 0x00, 0x00, 0x02, 0x00, 0x00, 0x00, 0x00, 0x10, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00};	

N.4 Browser Start (M1)

N.4.1 Browser Start (M1) example test vector 1

Table 177 provides an example of a Browser Start (M1) test vector.

Table 177. Browser Start (M1) example test vector 1

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery

Fields	Value	Note
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x04, 0x00, 0x00, 0x08, 0x28, 0x04, 0x01, 0x02	Bloom Filter elements: b:_ipp._tcp%nan b:_ipp._tcp%p2p
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x01, 0x0B, 0x00, 0x00, 0x00, 0x04, 0x00, 0x00, 0x08, 0x28, 0x04, 0x01, 0x02};	

N.4.2 Browser Start (M1) example test vector 2

Table 178 provides an example of a Browser Start (M1) test vector.

Table 178. Browser Start (M1) example test vector 2

Fields	Value	Note
AD length	0x19	25 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x15	21 bytes
Header	0x01	Bloom Filter Length: 20 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x02, 0x00, 0x00, 0x00, 0x20, 0x00, 0x21, 0x00, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x01, 0x00, 0x04, 0x00	Bloom Filter elements: b:_ipp._tcp%nan b:_ipp._tcp%p2p
Test vector (starting from the AD Type Code)	uint8_t m1_len20[] = {0x26, 0x02, 0x01, 0x15, 0x01, 0x00, 0x00, 0x02, 0x00, 0x00, 0x00, 0x20, 0x00, 0x21, 0x00, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x01, 0x00, 0x04, 0x00};	

N.4.3 Browser Start (M1) example test vector 3

Table 179 provides an example of a Browser Start (M1) test vector.

Table 179. Browser Start (M1) example test vector 3

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x01	Frame role: Seeker Only Transport State: Off
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes

Fields	Value	Note
		Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x28, 0x04, 0x00, 0x02	Bloom Filter elements: b:_ipp._tcp%nan
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x01, 0x0B, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x28, 0x04, 0x00, 0x02};	

N.5 Provider Responds to Browser (M2)

N.5.1 Provider Responds to Browser (M2) example test vector 1

Table 180 provides an example of a Provider Responds to Browser (M2) test vector.

Table 180. Provider Responds to Browser (M2) example test vector 1

Fields	Value	Note
AD length	0x0F	15 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x0A	Frame role: Provider Only Transport State: ON
Transport Data Length	0x0B	11 bytes
Header	0x00	Bloom Filter Length: 10 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x40, 0x00, 0x00, 0x80, 0x01, 0x04, 0x00, 0x00, 0x00	Bloom Filter elements: p:_ipp._tcp%nan
Test vector (starting from the AD Type Code)	uint8_t m1_len10[] = {0x26, 0x02, 0x0A, 0x0B, 0x00, 0x00, 0x40, 0x00, 0x00, 0x80, 0x01, 0x04, 0x00, 0x00, 0x00};	

N.5.2 Provider Responds to Browser (M2) test vector 2

Table 181 provides an example of a Provider Responds to Browser (M2) test vector.

Table 181. Provider Responds to Browser (M2) example test vector 2

Fields	Value	Note
AD length	0x19	25 bytes, excluding AD length field
Transport Discovery Data AD Type Code	0x26	
Organization ID	0x02	Wi-Fi Alliance Generic Service Discovery
TDS Flags	0x0A	Frame role: Provider Only Transport State: ON
Transport Data Length	0x15	21 bytes
Header	0x01	Bloom Filter Length: 20 bytes Channel Information: Not Present
Bloom Filter	0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x04, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x80, 0x00, 0x00	Bloom Filter elements: p:_ipp._tcp%nan

Fields	Value	Note
Test vector (starting from the AD Type Code)	uint8_t m1_len20[] = {0x26, 0x02, 0x0A, 0x15, 0x01, 0x00, 0x00, 0x00, 0x01, 0x00, 0x00, 0x04, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x80, 0x00, 0x00};	