ANNEX J GENERAL REQUIREMENTS FOR ENHANCED MEDIA-ACCESS-CONTROL (MAC) CAPABILITIES (Informative)

The channel-access control capability of STANAG 5066 Annex B Edition 1 provides mechanisms (i.e., the CAS-1 linking protocol) to establish a point-to-point link (or links) for data communication. The CAS-1 protocol belongs to the class of link request/accept protocols that are effective at resolving the hidden-terminal problem in wireless point-to-point scenarios, by ensuring peer communication only.

This annex introduces modes for enhanced media-access control capability for HF data communication networks, and the prescribed method in which they are used with other STANAG 5066 capabilities. These channel-access modes extend or modify, but do not replace, the channel-access and link-control mechanisms defined in Annex B of this STANAG.

Enhanced Media-Access Control capabilities are defined in the context of an augmented model of the HF Subnetwork's protocol stack shown in Figure J-1.

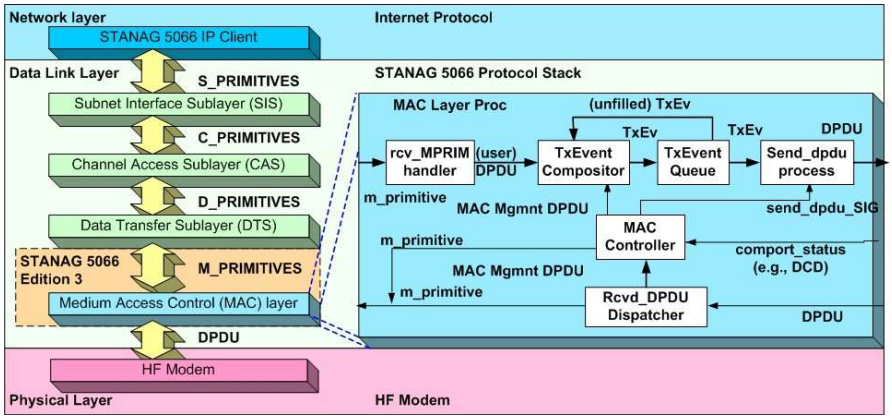

Figure J-1 — Augmented Model of the HF Subnetwork Protocol-Stack

The augmented model adds a Media-Access Control Sublayer (MACS) and inserts it below the Data-Transfer Sublayer of Annex C. Additional functionality implementing enhanced media-access control may be contained in the MACS, as shown in the figure.

The added media-access-control functionality:

- **shall** be based on the D_PDU message types defined in STANAG 5066 Annex C, and
- **may** use in addition new D_PDU types implemented for media-access control that **shall** conform to the message-definition rules and the Generic D_PDU Frame Structure and D_PDU field-element requirements of S'5066 Annex C Sections C.3.1 and C.3.2. New functionality to implement enhanced media-access-control **shall** be confined to the D_PDU Type-Specific Header element and, if present, D_PDU Payload element of any new D_PDU type.

To minimize impact on pre-existing functionality defined in Annexes A, B, and C for other layers of the HF subnetwork, new D_PDU types defined for media-access control **shall** only support peer-to-peer MACS-layer communication between nodes.

Node-to-node communication between HF subnet clients and peer-layer-to-peer-layer communication supporting the functionality of Annexes A, B, and C **shall** continue to use the D_PDU types defined in Annex C. The S_PDU and C_PDU specifications of Annex A and Annex B **shall** be unchanged by the MACs functionality.

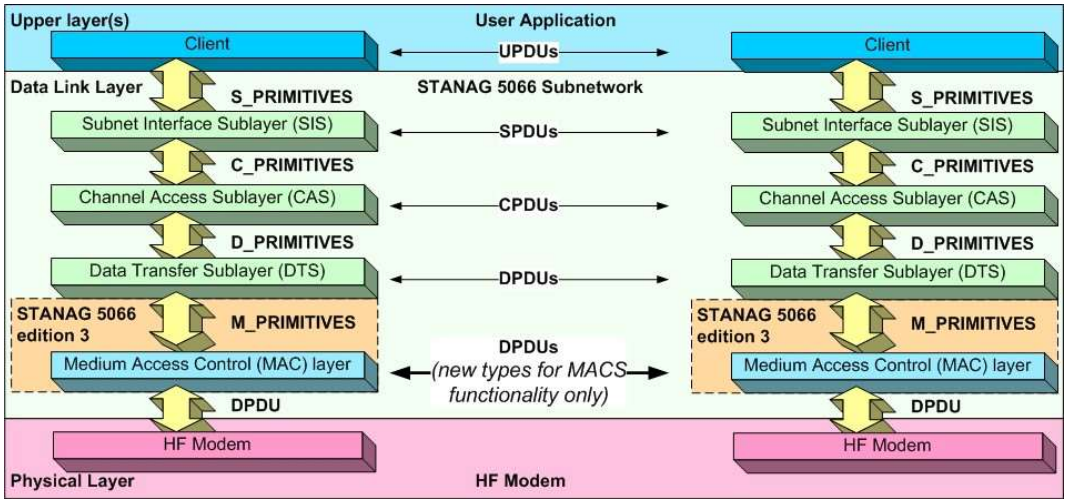

Figure J-2 — Peer-to-Peer Communication for Enhanced Media-Access Control

MACS functionality may be tailored as outlined in section J.3, which defines options to implement a range of functionality for multi-node networks. Detailed functional and performance specifications from other Annexes are cross-referenced where appropriate.

Four Media-Access Control Modes are defined:

1. Point-to-Point Mode (P2P)
2. Carrier-Sense Multiple Access (CSMA) Media Access
3. Wireless Token-Ring Protocol (WTRP) Media Access
4. Adaptive Time-Division Media Access (ATDMA)

These modes are summarized below. Implementation and performance requirements for these are standardized in the cross-referenced annexes.

J.3.1 Point-to-Point (P2P) Media-Access Mode

The point-to-point (P2P) media-access mode enables two nodes to reserve the channel for their use in point-to-point communication. The default point-to-point channel- access control **shall** be implemented in accordance with STANAG 5066 Annex B. It **shall** also use CSMA following STANAG 5066 Annex K, noting that for two nodes only some simplification of that Annex K procedure is possible.

J.3.2 Carrier-Sense Multiple Access (CSMA) Media-Access Mode

The Carrier-Sense Media Access (CSMA) mode enables a set of nodes to share the channel in a multi-node network. CSMA is a form of media-access control based on a node's ability to listen to the channel (i.e., radio-frequency carrier) and use its local knowledge that the channel is clear to control its transmissions to avoid interference — also called collisions — with the transmissions of other nodes.

If a CSMA mode is implemented, it **shall** be implemented in accordance with STANAG 5066 Annex K.

The CSMA mode specified in Annex K conforms to the requirements of this Annex: it is implemented using only the message catalogue defined by STANAG 5066 Edition 1, and the basic capabilities of Annexes A, B, and C, with augmented requirements for Annex D to implement a Listen- Before-Transmit (LBT) mechanism with collision avoidance.

J.3.3 Wireless Token-Ring Protocol (WTRP) Media-Access Mode

The Wireless Token-Ring Protocol (WTRP) media-access mode enables a set of nodes to share the channel in a multi-node network. Token-ring or token-bus multiple access is a form of media-access control based on ownership of a 'token' that grants the right to transmit (RTT) on the channel. A token holder transmits until it no longer has data to send, or until its right-to- transmit timer expires, and then it passes the RTT

token to its successor. Adaptation of each node's allocated channel capacity to the offered traffic load occurs automatically with the WTR mode.

The Wireless Token-Ring Media-Access mode **shall** be implemented in accordance with STANAG 5066 Annex L. The Wireless Token-Ring Protocol (WTRP) defined in that Annex is in two parts:

- a D_PDU message design for the management tokens exchanged by network nodes, and
- the algorithms used to create, maintain, and repair the ring (i.e., transmission sequence) of nodes in the network.

WTRP's D_PDU message design conforms to the requirements of this Annex. It uses new D_PDU message types based on EXTENSION D_PDU that conforms fully to the requirements of Annex C, whose D_PDU- specific part provides the requisite data fields to satisfy the information exchange requirements of WTRP.

J.3.4 Adaptive Time-Division Media-Access (ATDMA) Mode

The Time-Division Media-Access (TDMA) mode enables a set of nodes to share the channel in a multi-node network. TDMA divides the channel access into timeslots that are allocated to nodes in the network (or, even more generally, allocated to network services).

Fixed TDMA protocols are known to be inefficient in channel utilization and service times when the traffic offered by the timeslot owner (i.e., the node or service to which the time slot is allocated) is mismatched to the channel capacity provided by the time slot. This is particularly true when the node or service has insufficient offered traffic to fill the timeslot(s) it has been allocated.

Adaptive TDMA (ATDMA) permits variations in the timeslot allocation or length that allow the network to adapt to variations in the traffic offered by nodes and in their service requirements. To use ATDMA's adaptivity with STANAG 5066 would require new D_PDU management message types with which nodes coordinate timeslot usage and length information.

There is currently no STANAG 5066 Annex that specifies TDMA or ATDMA.

Through their conformance with the generic D_PDU-message structure defined in Annex C the enhanced media access protocols defined and cross-referenced herein are compatible in the limited sense that their common message elements (e.g., Maury-

Styles synchronization preamble, D_PDU type field, address fields, etc.) are recognizable regardless of which MACS mode is in operation or has been implemented by the node. Thus, all STANAG-5066-compliant implementations will be capable of decoding the field elements common to all the D_PDU messages. And, in particular, all compliant implementations will be capable of determining the source address of the node that sent the D_PDU and the type number of the D_PDU that was sent, even if the node does not implement the MACs protocol for which the D_PDU is used.

But the enhanced media access modes defined herein are not interoperable. There is no intent or expectation that a node implementing one of these enhanced media-access modes should be interoperable with a node implementing a different protocol. Rather, the intent and expectation is that standard operating procedures for network establishment will ensure that only nodes using the same media-access control protocol are network members. As this is a naïve view of what can happen in an operational network, this Annex defines provisions for nodes to discover the MAC-mode in use by other nodes, to, at the very least, recognize when they are using incompatible protocols and to take appropriate action to avoid mutual interference.

J.4.1 MAC-Mode Discovery

The processes by which nodes discover the media-access-control modes in use within a STANAG 5066 network are called MAC-Mode Discovery.

Nodes **should** implement MAC-Mode Discovery, which consists of the process elements defined here:

- Use of D_PDU Type 15 Warning Messages – the (mandatory) provisions of Annex C Section C.3.12 **shall** apply to the implementation of MAC-Mode Discovery, as further amplified below.
- Channel Analysis – nodes implementing a given media-access mode shall analyze the channel usage by other nodes to detect violations of the protocol that it implements, and take actions as noted further below. These actions include the use of Type 15 Warning messages to notify neighbouring nodes of the protocol incompatibility.

J.4.1.1 Use of Type 15 Warning Messages

A STANAG 5066-compliant node that receives a D_PDU message that is “unexpected or unknown” to it is required under the provisions of Annex C Section C.3.12 to send a Type 15 D_PDU (Warning) Message to the node that generated the unexpected or unknown D_PDU. This requirement is unchanged by the enhanced-media-access modes defined herein.

In particular, and with cross reference to Annex C Section C.3.12, a node that receives a D_PDU that is unexpected for the MACS protocol is it is using (this may be an indication that the sending node is using a different MACS protocol) or that unknown to it (also a potential indication of an incompatible MACS protocol) will determine the source address of the node that sent the unexpected or unknown D_PDU and send a Type 15 D_PDU (Warning) Message to that node:

- As required in Annex C, the Type 15 D_PDU (Warning) Message RECEIVED FRAME TYPE field **shall** indicate the Type number of the unexpected or unknown D_PDU.
- If the node does not recognize the received D_PDU, the Type 15 D_PDU (Warning) Message REASON WARNING SENT field **shall** be set to the value assigned to the reason “Unrecognised D_PDU type Received”.
    - N.B.: This case applies to D_PDU types with subtypes, i.e., the Type 6 D_PDU (Management) that uses the Engineering Orderwire (EOW) Type field (as defined in Annex C) as a subtype indicator to distinguish variants of the Extended Management Message types: the receiving node may recognize the main type (i.e., Type 6 Management Message) but not the subtype (i.e., the particular Extended Management Message subtype designated by the EOW-type field type). In this case, the node **shall** treat the D_PDU as an unrecognized D_PDU, and send a Type 15 D_PDU (Warning) Message as above.
- If the node recognizes the received D_PDU, but it was unexpected for the protocol that it was using, the Type 15 D_PDU (Warning) Message REASON WARNING SENT field **shall** be set to the value assigned to the reason “Invalid D_PDU Received for Current State”.
    - N.B.: This case also applies to D_PDU types with subtypes as described in the preceding case. If the node receives a D_PDU of the proper type but if the subtype is unexpected, e.g., it designates an Extended Management Message defined for a MACS protocol that the node recognizes but is not currently executing, then in this case also, the node **shall** treat the D_PDU as an unexpected D_PDU, and send a Type 15 D_PDU (Warning) Message as above.

- In particular, a node executing the P2P or CSMA mode that receives any of the new D_PDU types defined in Annex L (for WTRP) (whether or not they are recognized to the receiving node) **shall** send a Type 15 D_PDU as specified

above.

Use of Type 15 D_PDU (Warning) Messages of course is possible only when the node is configured in a compatible transmission mode; nodes configured for transmit-only operation (e.g., to providing exclusive support to a Broadcast Data Exchange Session as defined in Annex A) will not receive any D_PDUs that could trigger the warning condition, and nodes configured for receive-only operation (e.g., to receive the Broadcast Data) would not be capable of sending the warning messages and therefore disable the protocol-error-detection logic and warning-message- generation functionality.

J.4.1.2 Channel Analysis

Transmissions by nodes executing one MAC-mode will likely be uncoordinated with the transmissions of nodes executing another (i.e., they don't participate in the protocol), and mutual interference may occur.

Nodes executing a given MAC-mode **shall** analyze the D_PDU messages received from other nodes to detect violations of the protocol it is executing. Message analysis includes the following:

- processing of received Type 15 D_PDU (Warning) Messages in accordance with Annex C and as amplified by Section J.2.1.1.
- analysis and identification of the MAC mode in use by other nodes:
    - transmissions that contain none of the new D_PDU types (recognizable to the receiving node) defined in Annex L (for WTRP) **should** be assumed to originate from a node that is currently operating in P2P or CSMA modes, as these modes (i.e., P2P and CSMA) do not use any new D_PDUs for their operation. This indication is one of the current operating mode, and not of capability.
    - Transmissions that contain Type 15 D_PDU (Warning) Messages that warn ignorance of any of the new D_PDU types defined in Annex L (for WTRP), i.e., that have a RECEIVED FRAME TYPE field defined for one of the new D_PDU types and that denotes a REASON WARNING SENT field as unrecognized, **should** be assumed to originate from a node that is capable of operating only in P2P or CSMA modes. The presumption **should** be that node is a legacy (STANAG 5066 Edition 1 compliant) implementation incapable of executing either WTRMA or ATDMA.

- Transmissions that contain Type 15 D_PDU (Warning) Messages that warn of unexpected use of any of the new D_PDU types defined in Annex L (for WTRP), i.e., that have a RECEIVED FRAME TYPE field defined for one of the new D_PDU types and that denotes a REASON WARNING SENT field as unrecognized, **should** be assumed to originate from a node that is operating in a different MACS mode than the node to which the Type 15 D_PDU (Warning) Message is addressed.

J.4.2 Embedding Broadcast / Multicast Traffic

Receive-only nodes (e.g., nodes in an emission-control [EMCOM] status) make no transmissions that can interfere with the operation of multi-node network, whatever MACS mode it uses. This may be exploited by nodes that do transmit in a multi-node network to embed broadcast or multicast traffic, a capability that is fully consistent with the intent of Annex A Section A.1.1 (from Edition 2 and later of this STANAG).

The MAC layer **may** be mapped onto the underlying HF channel in one of the three ways set out below.

J.5.1 Fixed Frequency

In this mode, a fixed frequency agreed by all nodes is used. If STANAG 5069 Wideband HF is used, a fixed bandwidth is also chosen. This **shall** be the same for all nodes on the network. This is a simple and robust choice that is effective for some deployments, such as a network using HF surface wave.

J.5.2 Scheduled Frequency

A variant on fixed frequency is to have an agreed schedule of frequency use that is followed by all nodes. This can allow for adaptation to conditions in a simple manner, for example to use different daytime and nighttime frequencies.

J.5.3 ALE for All Nodes

STANAG 5066 Annex B defines channel access mechanisms that set up ALE links on demand for point to point and multicast links.

An alternate approach is to use ALE for all nodes on the channel, which is managed at MAC layer. By maintaining an open channel, it enables all nodes on the channel to

communicate with CSMA or WTRP. It will prevent the situation where a pair of nodes are connected on a channel, which blocks communication with other nodes.

Use of ALE at MAC level means that a channel can be kept open for all nodes and that the best channel at a given time can be chosen. It is important that the ALE channel is closed and re-opened from time to time, in order to ensure choice of best channel and to bring on nodes that were not available on the previous ALE setup.

1. Changed to include networks of any number of nodes. Edition 3 title and introduction suggest multiple nodes, but this is contradicted by much of the text which covers two node networks.
2. Removed normative references to Annex M, which is a placeholder.
3. Require use of CSMA for point to point. Edition 3 notes that MACS adds no functionality which is contradicted by footnote explaining why MACS should be used.
4. Added section on mapping to channel and use of ALE.