Tutorial on 802.11 MAC Formal Description

Michael Fischer
Digital Ocean, Inc.

Objective

To generate an unambiguous description of the 802.11 MAC behavior, with particular attention to:

- the reference points for measuring the various timed intervals;
- the scope of interpretation for each header field, service interface parameter, and MIB attribute, and the specific meaning of each value for enumerated types;
- interactions between different functions that may apply to the same data units or time intervals — with explicit prioritization among these functions where necessary;
- the situations that yield each status or reason code; and
- MAC response boundary conditions, especially the results which arise when one party to communication over the wireless medium is not following the specified protocol or when a pair of stations are attempting to communicate while having different local views of the medium, station, or service set state.

Feedback — how does the D5 text look in retrospect

We did a good job of describing the desired functionality.

We did a reasonably good job on anticipated expception conditions:

- There are some exceptions which can be detected but not reported.
- There are some status codes with no detectable cases for their use.

We did a good job of providing for reasonable behavior in the presence of unanticipated responses or inputs, but many of those provisions are implicit, or not clearly identified in the text.

We allowed significant inconsistencies, expecially at the MAC/PHY interface and in the definition vs. usage of MIB attributes.

We did a poor job of specifying the interactions between different categories of functions (e.g. IBSS power management and the DCF access mechanism, scanning and MAC data service), the sources of certain types of control information, and the operational boundary conditions.

- The boundary is HUGE.
- ... (at times the shape of the boundary appears to be a fractal curve) ...

General Approach

1. Group functions into state machines to match defined function sets visible at an exposed interface.
2. Show time-related actions explicitly, including those dependent on the absence of events (e.g. response timeouts) and those measured in derived units (e.g. backoff "time" in increments of idle slots).
   - The most important MAC characteristics observable on the WM concern the use of time and many decisions critical to interoperability are made based on the state of the medium at the ends of specified time intervals.
   - SDL has excellent facilities for managing time, and enforces the distinction between absolute time (Time sort) and relative time (Duration sort).
3. Emphasize communication-related functions in the state machine diagrams by encapsulating the encoding and manipulation of frames, fields, and ancillary data structures with their data type definitions.
   - This approach, which relies heavily on SDL's abstract data type and inheritance mechanisms, permits the behavior of the data-holding entities to be precisely defined, without adding excessive complexity to the process diagrams.

Global Assumptions for State Machine Operation

- State transitions and tasks within processes require zero time.
- Signals between processes are transferred instantaneously.
  - Thisis always true of signal routes within SDL blocks.
  - All inter-block channels are defined as non-delaying channels.
  - All remote variables and procedures are declared with the 'nodelay' property.
- One unit of system time represents 1 microsecond of MAC operation.
  - Functions Usec and Kusec are defined to perform any necessary conversions.
- Where feasible, Z.105-like constructs are used to facilitate integration of the SDL MAC description and the ASN.1 MIB description prior to finalization of the standard.

Extended Notation Conventions

- Sorts (data types) use names beginning with capital letters, variables and named constants use names beginning with lower case letters.
- Names beginning:
  - with lower case "s" are static data values (named constants) globally available to all blocks;
  - with lower case "m" are exported variables needed by various portions of the MAC, but not part of the MIB (which uses names beginning with lower case "a");
  - with lower case "t" are times (timers use "T"); and
  - with lower case "d" are durations.
- To help fit text into the SDL graphical symbols, only the first characters of acronyms are capitalized in most cases (e.g. Msdu).
- Page names appear to be giberish — they are selected to cause the files containing individual pages to appear in the correct order under DOS/Acrobat 8.3 file name constraints.

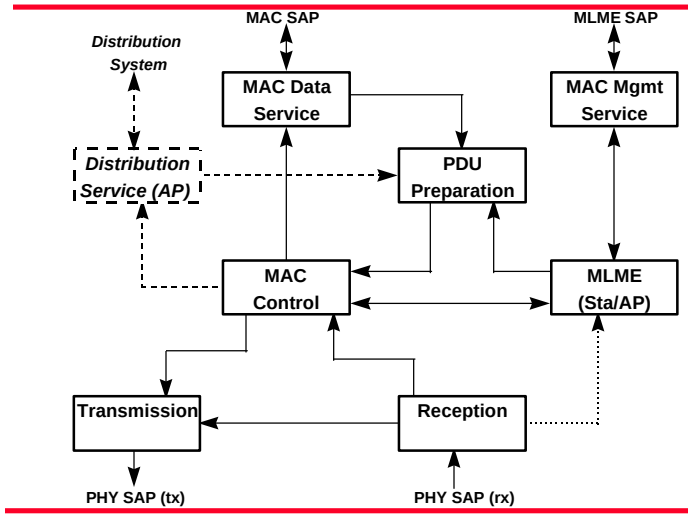
Data Unit Modeling

- The fundamental unit of data unit representation is the bit
  - Bits are a subtype of SDL's Boolean sort. "0" and "1" are literals, and do not have integer-compatible values.
- A Bitstring is a 0-origin string of bits
  - SDL strings are 1-origin. The string0 generator is adapted from Z.105.
  - Bitstrings support bitwise boolean operations (and, or, xor, not).
- An Octet is a Bitstring of {nominal} length 8
  - Z.105 extends SDL's syntax to allow a 'size(8)' property, but for now we have to rely on proper usage to ensure that Octets stay 8 bits long.
  - octetVal(Octet) converts an Octet to an Integer [0:255].
  - mkOctet(Integer) converts an Integer mod 256 to an Octet.
- An Octetstring is a 0-origin string of Octets
  - This is very handy for 802.11 frame formats, but Z.105 (ASN.1) Octetstrings are 1-origin, so we may need to rename this type.
  - The Frame sort is a subtype of Octetstring with operators to extract and modify all header fields and most management frame body fields.

Data Unit Transfer Modeling

- The formal description is a DESCRIPTION of normative behavior, and does NOT attempt to describe implementation!
  - There are numerous instances where the techniques used would be exceedingly ineficient to implement, even if the "zero processing time" assumption could be accommodated in a working implementation.
- Individual and collective data unit structures are conveyed between blocks as signal parameters.
- Queues are defined using a variant of SDL strings
  - The queue generator is a slightly modified version of the string0 generator which adds operators to add an item as the first (Qhead) or least (Qtail) element.
  - A Qsearch operator is available to select elements on a queue by content.
  - Length(queue) can be used to determine the depth of a queue.
  - Transmission-related queues are defined as strings of the "FragSdu" data structure.

Functional Decomposition



MAC Data Service

Provides the service interface to LLC

- **Validates MaUnitdata.request, adds MAC header, and sends to PDU preparation.**
  - **priority=contention-free with no point coordinator reports unavailable priority and sends in contention period**
  - **Only "undeliverable" is available as a status code if the initial request is valid. Several distinct errors, including noBss, not authenticated, not associated, excessive retries, and transmit lifetime exceeded, are reported as "undeliverable" for now.**
- **Reports received MSDUs with MaUnitdata.indication.**
  - **The status code is always "successful".**
  - **The provided priority is actually the priority of the last fragment.**

MAC Management Service

Maintains the MIB and provides the MLME service interface.

- MIB attributes are modeled as remote variables, exported by the process which creates or provides the value (process MIB for read-write or write-only attributes).
- MIB process also contains some intra-MAC remote variables needed as a result of the MIB simplification.
- MLME requests are filtered for validity under station capabilities and operating state prior to being passed to the MLME block.

Distribution Service (AP only)

This block provides an interface between the intra-BSS frame handling and the distribution system medium.

- Due to the minimal definition of the DS, and the lack of a service interface to the DS, most of this block is informal text.

PDU Preparation

Performs fragmentation, encryption, power save and contention free queueing, and transmit life timing.

- All transmissions using the basic access mechanism go through PDU preparation:
  - MSDUs from MAC Data Service,
  - MSDUs from Distribution Service (at APs), and
  - MMPDUs from MLME.
- The incoming MSDU/MMPDU is transformed into an instance of the FragSdu structure containing an array of fragments plus the per-MSDU information such as retry counts, transmit lifetime, and current fragment number.
- Encryption needs to be done along with fragmentation because the MPDU size is affected.

MAC Control (DCF and CF-responder)

Provides DCF and CF responder (if CF-pollable). On transmission:

- generates Rts if length > aRtsThreshold,
- performs CTS timeout and handles backoff and retry,
- performs ACK timeout and retry, as well as backoff after successful transmission,
- cancels pending transmission at TBTT (in IBSS).

On Reception:

- generates ACK for valid receptions and when Reception block has signalled "need ack" for discarded duplicate or ICV error,
- CF-poll response, including detection of cases needing response of CF-Data+Ack (if CF-pollable),
- class 2 and class 3 error detection and reporting, and
- reassembly (with receive lifetime processing).

Management frames are routed to MLME block, completed MSDUs are routed to MAC Data Service.

MLME (for non-AP Station)

Performs

- scan,
- join,
- beacon generation and dwell timing,
- (re/dis)associate, including class 3 error reporting,
- (de)authenticate, including class 2 error reporting,
- start IBSS, and
- monitoring of station & power save state.

MLME (for AP)

Performs

- start BSS,
- beacon generation and dwell timing,
- (re/dis)associate response,
- (de)authenticate response,
- point coordination (if CF option implemented and active), and
- monitoring of station & power save state.

Transmission

Includes backoff and timestamp insertion.

- If MPDU passed down using TxRequest, delays transmit based on medium busy and unexpired backoff count.
  - These transmissions may be cancelled if not yet started by issuing a TxCancel signal.
- If MPDU passed down using TxImed, initiates transmission at the specified absolute time, without concern for medium state (for SIFS responses such as ACK, CTS, etc.)
- CRC is generated during transmission and appended to MPDU (with PLCP length preincremented by 4 to accomodate this field).
  - If the frame type is Beacon or Probe Response, the timestamp field value is inserted into octets 24-31 during transmission (with precompensation for PHY Tx delay).

Reception

Performs receive filtering and channel state monitoring:

- CRC and PLCP length verification,
- NAV update from duration value and CF parameter set element when appropriate,
- RA/DA matching and BSSID matching when DA is group address,
- duplicate filtering and maintenance of tuple cache,
- decryption and removal of IV and ICV fields if WEP bit is on (or discarding of frame if ICV does not check),
- receive MIB counter update,
- power save bit test and reporting to power save monitor process,
- maintaining the NAV and RTS timeout timers, and
- reporting of busy/idle state and slot boundaries to transmit block with proper relationship to PhyRxend.indicate.