



DECT NR+ PROTOCOL STACK · NORDIC SEMICONDUCTOR nRF9151

BFi91NR7DLCVG

ETSI specifies MAC, DLC and Convergence separately; we build them as one whole — one radio timeline, one set of counters, one service surface. Written to ETSI TS 103 636 V2.2.1 (Release 2), running on the Nordic Semiconductor nRF9151. **The stack is not sold on its own; it comes with BANFi's development services:** we load it onto your board, turn your specification into a manufacturable product, and measure on your hardware until the numbers are ones you can stand behind.

TS 103 636

V2.2.1 · RELEASE 2

MAC → CVG

THREE LAYERS AS ONE

Static

MEMORY POOLS · NO
HEAP ON THE DATA
PLANE

Mode 1

AES-128 LINK SECURITY
· WHEN ENABLED

1.9 GHz · 915 MHz

LICENCE-EXEMPT ·
ONE IMAGE

Measured on the reference build

24–33 ms

Triggered handover (25 of 25 handovers)

Make-before-break, source link held throughout; checked against a no-handover control.

541 µs

Security processing per PDU

AES-128 CMAC integrity and AES-128 CTR ciphering, hardware-accelerated.

~4 s

Cross-channel discovery to join

A device that wakes on the wrong channel finds the cluster and joins it by itself.

373 kbit/s

Star uplink in aggregate

Two full-rate children at once; a single granted link carries about 201 kbit/s each way.

Depth 5

Mesh tree, verified

Nine radios, every node to every other both ways, up to six hops from source to destination: 350/350 unicast delivered.

47.0 ms

Round trip between source and destination (secured)

The application echo floor, with the link secured and under contention.

Every platform measures differently. These figures come from our reference build on the nRF9151 and move as the stack evolves; silicon revision, build configuration, clock and power settings, antenna and RF environment, host interface and your own application load all shift them either way. They are not protocol conformance results and carry no regulatory meaning.

Mobility, handover and loss are three different things

24–33 ms

Triggered handover, make-before-break — and only the last step: the neighbour is already tracked and the decision has been taken.

< 60 s (worst observed)

Cold start to handover. From an empty probe list: probe-arm, neighbour discovered, trigger, and only then the millisecond switch above.

20 s + one recapture

Unannounced loss of the serving side. The failure path, not a handover: ten missed beacon periods declare the loss, then one recapture step restores the association; in-flight unacknowledged frames are the only data loss.

Failure semantics

A link that silently loses messages is fine for telemetry and useless for anything that must act on what it receives. The stack is built so that the layer above always knows where it stands.

Exactly one result per send

Every accepted send returns one delivery result — not zero, not two. An application never infers from a timeout whether something arrived.

No silent-drop path

No code path discards a packet without reporting it. Any loss is visible, with a reason, everywhere it can happen.

Integrity verified on air

Security Mode 1 verified on captured traffic. A 45-minute secured soak across five carrier moves and five secured re-associations recorded zero MIC failures.

Counters survive reboot

Cipher counters stay unique across power cycles, so a restarted device never reuses a spent keystream — measured on the ciphertext.

Protocol capability

MAC (TS 103 636–4)	Fixed and portable termination roles, or both at once as a mesh relay. Random and scheduled access; HARQ with closed-loop feedback, redundancy-version rotation and bounded give-up. Automatic neighbour tracking, count-to-trigger and make-before-break handover.
DLC (TS 103 636–5)	Segmentation, reassembly and lifetime control; implicit ARQ from HARQ outcomes. Uplink, downlink, hop-budgeted flooding and source routing; cached downlink routes repair themselves.
Convergence	Flow-control windows and ARQ with segment-level NACK; Endpoint and Mux-Tag multiplexing; duplicate removal, in-sequence delivery, segmentation and reassembly.
Security	Security Mode 1 (AES-128 CMAC + CTR), hardware-accelerated, when enabled: hop-by-hop link security on the MAC, and optional per-flow payload security at the convergence layer, which keeps payload encrypted across relays that hold no key for it (verified to depth 3).
Bands	1.9 GHz (band 1) — every measurement in this brief. 915 MHz (band 4) — protocol behaviour air-verified with the same image; throughput and range not yet characterised. The band group is a run-time parameter.
Test specification	Full TS 104 047–2 suite on the shipping image: 48 pass, 5 pass with comment, 2 not applicable (own bench, 2026–09–14). All 8 DLC and all 4 Convergence purposes pass.

Two ways into your product (brought in by BANFI's development services)

Embedded API — on the nRF9151 itself

Your application runs on the SiP's own Cortex-M33 beside the stack. One part, one image; the memory left for your code depends on the role and is given per mode in the full specification.

HIF-UART / HIF-SPIS — beside your own MCU

Your MCU keeps its architecture, toolchain and application; the radio becomes a peripheral it reads and writes. UART at 1 Mbaud or SPI slave, one CRC-16-protected register interface; a host driver of about 150 lines.

Resources, capacity and link budget

Memory	Static pools sized per role; no heap on the data plane, so what a build uses is also its worst case. Memory tables per mode are in the full specification.
Per fixed termination	A 64-device roster; with the shipping schedule, 3 full-rate data channels, the rest joining as RACH members with a usable uplink (about 4 SDU/s at 20 bytes).
Throughput	About 201 kbit/s each way on one granted link (250-byte payload, ~100 per second); star uplink 373 kbit/s in aggregate; 96–101 per second per routed hop (depth 1–3).
Link budget	No kilometre figures. Thresholds measured in a two-storey house: full-rate data –75 dBm, throttled data –82 dBm, association lost at –82 to –85 dBm; transmit power up to +21 dBm (subject to local regulation).
Target platform	Nordic Semiconductor nRF9151 System-in-Package (mixed meshes with nRF9131 also verified).

Known boundaries

- Relay depth is verified to 5 (nine radios, up to six hops from source to destination); deeper topologies have no on-air evidence yet, so plan a pilot rather than a production deployment beyond that. Per-flow payload security at the convergence layer is verified to depth 3.
- Throughput and range on 915 MHz are not characterised: the bench antennas are 1.9 GHz parts.
- Not submitted for formal conformance testing; no regulatory approval or interoperability certification. The test functions certification needs (test loop, CW source, monitor mode, ETF) are built in and bench-verified.
- No functional-safety claim. It provides the properties an IEC 61508-style black channel needs from the transport, so an application-level integrity protocol can make its own claim.
- What has accumulated so far is hours of continuous and instrumented running, not months of field deployment.

How to get it

The stack is not sold or licensed on its own; it comes with BANFI's development services — loaded onto your board, built into your product, measured on your hardware. The full specification (memory tables per mode, timing tables backed by test reports, clause-coverage audit, integration guide and host register map): leave your company details in the enquiry form at banfiww.com and choose "Full specification and integration documents".