Snadné nasazení IQRF® s IQRF OS 4.03D

Nový operační systém IQRF OS 4.03D s sebou přináší řadu vylepšení, která by vám měla usnadnit práci se sítí IQRF. Jsou to zejména funkce **Smart Connect** a **Autonetwork V2**.

# Smart Connect

Jedná se o novou metodu přidání Nodu do sítě IQRF.

## Vlastnosti

* Nod nemusí být v přímém dosahu Koordinátoru, ale pak musí být v dosahu Nodu, který je již k dané síti přibondován.
* Na straně bondovaného Nodu není potřeba žádná akce (např. stisk tlačítka).
* Bondovaný Nod **nemusí** mít v konfiguraci nastaven pracovní **kanál**, ani **Access Password** dané sítě.
* Smart Connect je založen na systémové komunikaci šifrované pomocí **IBK** (Individual Bonding Key). Jedná se o unikátní a neměnný kód uložený v každém TR modulu během výroby.
* Aby mohl Koordinátor přidat daný Nod do sítě, musí znát jeho IBK a MID (Module ID).

**Smart Connect** je implementován v DPA jako nový příkaz periferie *Coordinator*. HWP Nodu podporuje „tlačítkové bondování“ a současně i Smart Connect.

V odbondovaném stavu (na Nodu bliká červená LED) je Nod v LP příjmu (nízká spotřeba) a očekává systémový *Smart Connect* paket. Pokud je stisknuto tlačítko, Nod odesílá požadavky na přibondování/předbondování. Pokud tlačítko stisknuto není, Nod po uplynutí času cca 5 hodin usne. Takto dlouhý čas nabízí prostor pro instalaci Nodů a spuštění procesu *Smart Connect*. Změna tohoto času je možná v *Custom DPA Handleru* (event *BondingButton*). Případně je možné zakázat spaní zcela pomocí konfiguračního parametru *Stay awake when not bonded*.

## Testování procesu Smart Connect

Proces *Smart Connect* lze spustit DPA příkazem *Smart Connect* zaslaným koordinátoru na periferii *Coordinator*. Hlavními vstupními parametry jsou **IBK** a **MID** bondovaného Nodu, a požadovaná logická adresa. IBK i MID lze zjistit aplikačně nebo v IQRF IDE – *TR Module Information* (Ctrl+M).

*Smart Connect* lze, jako každý DPA příkaz, testovat v IQRF IDE pomocí **terminálu** nebo uživatelsky přívětivěji pomocí **IQMESH Network Manageru**.

## Smart Connect v praxi

Vstupní parametry (IBK, MID) lze předat procesu *Smart Connect* pomocí tzv. **IQRF Smart Connect Code**. Jedná se o alfanumerický řetězec, ve kterém jsou zakódovány **IBK**, **MID** a **HWPID** (Hardware Profile ID) daného zařízení. Tento kód lze vygenerovat pomocí nástroje *IQRF Code Tool* v IQRF IDE nebo uživatelsky na základě dostupné dokumentace, a předávat různými způsoby, např. pomocí NFC, QR kódu atd. Nástroj *IQRF Code Tool* umožňuje i vygenerování QR kódu.

## V praxi pak *Smart Connect* může vypadat takto

* V IQRF IDE se každému TR modulu (Nodu) vytvoří QR kód a nalepí se na dané zařízení obsahující tento TR modul.
* Zařízení se umístí na své místo a pomocí mobilní aplikace (např. *IQRF Network Manager* pro Android) se načte QR kód.
* Mobilní aplikace je propojena s **IQRF Repository**, proto je schopna podle HWPID zjistit a zobrazit informace o zařízení (typ, výrobce, ovladače...).
* Mobilní aplikace se přes API spojí s bránou, na které běží **IQRF Gateway Daemon** a spustí službu **Smart Connect**.

## Jak je to s pracovním kanálem?

Od IQRF OS verze 4.03D probíhá veškeré bondování (Local – např. tlačítkem, Smart Connect, Autonetwork V2) na **servisních kanálech**. Bondovaný Nod tedy nemusí mít v konfiguraci předem nastaven pracovní kanál stejný jako Koordinátor sítě. Při instalaci sítě stačí nastavit vhodný (nezarušený) kanál v Koordinátoru a všechny přibondované Nody tento kanál „zdědí“ a uloží si jej automaticky do konfigurace během procesu bondování.

Výjimku tvoří Remote Bonding, resp. jeho část „předbondování“. Předbondování je poskytováno stávajícími Nody v síti, proces probíhá na pozadí na pracovním kanálu sítě a Nod, který má být předbondován, musí mít tento pracovní kanál předem nastaven v konfiguraci.

Čísla servisních kanálů uživatel nepotřebuje znát, nicméně jsou uvedena v dokumentu *IQRF OS User´s Guide* – mapa kanálů.

## Jak je to s přístupovým heslem?

V případě **Smart Connect** bondování **nemusí** být v konfiguraci bondovaného Nodu nastaveno stejné **Access Password** jako na Koordinátoru. K šifrování a autorizaci je použit **IBK** daného Nodu.

**Ostatní** způsoby bondování (Local např. tlačítkem, Remote, Autonetwork V2) použití stejného **Access Password** **vyžadují**.

Access Password je i nadále používáno pro autorizaci v *DPA Service Mode* (DSM) a k šifrování/dešifrování zálohy síťových dat během procesu *Backup/Restore* pro účely snadné výměny Koordinátoru/Nodu v síti (v případě potřeby).

# Autonetwork v2

Jedná se o novou verzi automatického sestavení sítě využívající služeb implementovaných přímo v operačním systému.

## Vlastnosti

* Na straně Nodu není potřeba žádný *Custom DPA Handler*.
* V Koordinátoru je nahrán *Custom DPA Handler* nezbytný pro funkčnost *Autonetwork* (*CustomDpaHandler-Coordinator-AutoNetworkV2-Embedded.c*)
* Nody **nemusí** mít nastaven **pracovní kanál** Koordinátoru. Kanál je „zděděn“ a automaticky uložen do konfigurace během procesu *Autonetwork*.
* Nody, které mají být přidány do sítě, musí mít nastaveno stejné **Access Password** jako Koordinátor.

Sestavení sítě probíhá ve vlnách. V každé vlně postupně probíhá:

* *Prebonding* (přidělení dočasné adresy 0xFE),
* *Authorization* (přidělení logické adresy),
* *kontrola* přibondovaných Nodů (nekomunikující Nody jsou v Koordinátoru odbondovány),
* *Discovery* (zjištění topologie sítě).

V první vlně jsou do sítě přidány Nody v přímém RF dosahu Koordinátora. V dalších vlnách se na sestavování sítě vždy podílejí také již existující Nody v síti. V případě, že během nastaveného počtu vln (defaultně 2), nedojde k přidání žádného nového Nodu, proces *Autonetwork* se ukončí.

Proces *Autonetwork* se spustí DPA příkazem určeným Koordinátoru, příkaz je dostupný například v makrech (pod názvem *Autonetwork embedded - Start*).

## Znázornění procesu Autonetwork V2

