Adventures in SWD

The goal!!!

- Flashing code
- Breakpoints!
- Watches!!!

Probes and CPUs

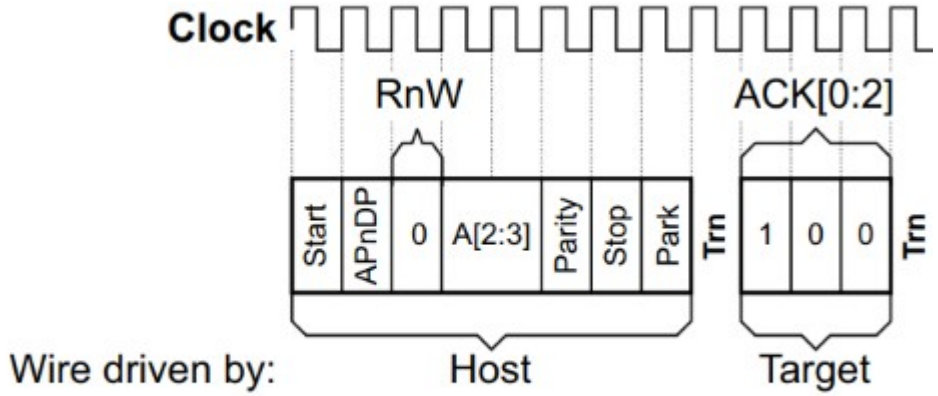
- ARM cpus are very common and all have similar interfaces
- SWD is arm proprietary
- Jlink and CMSIS-DAP are the common probe types. They both talk SWD but have bespoke USB/IP protocols

The DAP

- DP (Debug Port)
  - JTAG or SWD
  - Is ultimately a system for reading and writing registers
- AP (Access Port)
  - Memory Access port (MEM-AP)
  - Different types for different buses.

SWD Packets

- Bit-oriented protocol
- A packet contains a one byte "command", a 3 byte acknowledgement, and 32 bits of data.
- Command contains 2 bits of register address (A[2:3])
- Other bits of the register address are stored in a register named STATUS which is always written to when A[2:3] is 0b10.
- Command also encodes whether to access DP register or AP register and whether operation is a read or a write



Setup

- Reset into SWD mode
  - Some devices support SWD or JTAG and boots into a special mode that lets you choose (SWJ-DP)
  - Finished by reading DPIDR which identifies the DP
- Send ABORT to clear errors
- If an error is raised, all reads and writes will return Fault
- Power up the System and Debug through CTRL_STAT register

Reading and writing Memory

- Reading and writing are done through three AP registers
- CSW – Control/Status word for configuration (Data size, auto-increment, etc.)
- TAR – The address to read/write from
- DRW – The register to read/write to actually read/write the data

CoreSight

- All ARM processors contain a tree of components which are discoverable through a system called CoreSight
- Every MEM-AP contains a register called BASE which points to the first element
- Typically, this is a Rom Table which contains pointers to other elements
- Elements types range from general CPU control to breakpoints to tracing

DEMO TIME

Chat