Developers Conference 2007

Amsterdam, The Netherlands

Wireless USB 1.1 Additions and Improvements

Rahman Ismail
Sr. Software Architect
Intel Corporation

Focus Areas

- Wireless USB Additions/Modifications
  - Directed beaconing
  - Security and Loopback Updates
  - Control transfer boundary conditions
  - Wireless equivalent of HNP for DRD devices
  - Power efficiency improvements
- Association Model Update
  - Add support for NFC as an association method
- UWB Upper band support
- Includes current errata list

Security and Loopback Updates

- Improve user interface to provide the user a visual representation of the device being associated
  - Allow the Configuration descriptor to be queried in un-secure mode
  - Add the capability to return a bitmap/jpeg image of the device via the BOS descriptor
- Add the ability to test the bursting capabilities of a device
  - Only required to be supported on the endpoint that has the largest bursting capability
  - Compliance testing
    - Requires a special host
  - Checking the status of the channel

Control Transfer Boundary Conditions

- Case 1: ACK smashed

MMC	Dir	IE Id	CTA 0	# Notif TS's	CTA 1	Addr	Endp	EDir	bvDINAck	Data	CTA 2	IE Id	IE Id	FCS
	-->	WCTA_IE	DNTS	8	DT	128	0	IN	0x00000001	00 05 00 00 00 00 00 00	EOL	WCONNECTACK_IE	WHOSTINFO_IE	0x71F1FC91

Hand	Dir	Host Id	ACK	bvAckCode
	<--	0xAA55	1	0x00000001

ACK of status not received by host

- Case 2: MMC smashed

MMC	Dir	IE Id	CTA 0	# Notif TS's	CTA 1	Addr	Endp	EDir	bvDINAck	Data	CTA 2	IE Id	IE Id	FCS
	-->	WCTA_IE	DNTS	8	DT	128	0	IN	0x00000001	00 05 00 00 00 00 00 00	EOL	WCONNECTACK_IE	WHOSTINFO_IE	0x71F1FC91

- Lost MMC or lost data-in/handshake packet are not distinguishable
- Add a bit to the CTA in MMC stating that it is a retry of a previous Control Transfer

Wireless Equivalent of HNP for DRD Devices

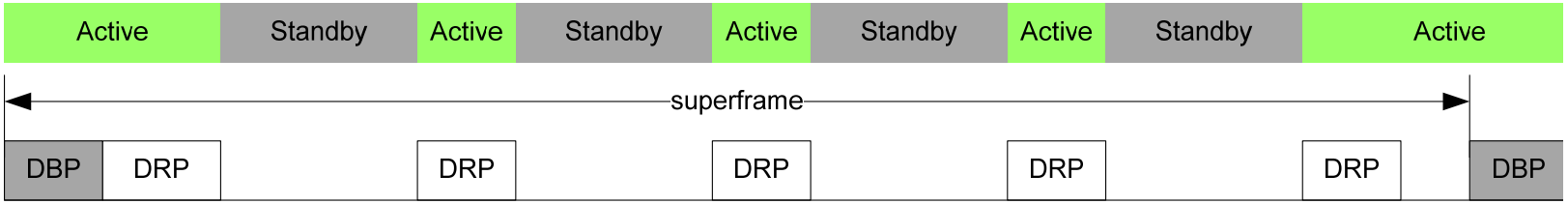
- Supporting Host and Device simultaneously is complex
  - Requires a lot of resources
  - Want to be able to reuse existing OTG stacks
- Host is selected using User input
- Devices can mutually agree to swap functionality
  - New DN_SWAP device notification
  - Requires an Acknowledgement (new SWAP_ACCEPT_IE)
  - Acknowledgement includes the time the device and host will switch capabilities
- A new SWAP Capable bit in the Host IE

Device Power Management
Existing Principles

- Devices and their drivers own device PM
  - Just like the wired case for selective suspend
  - Hosts don’t need to manage devices to save host power
- Three ways to save power
  - Conserve during normal operation
    - Shut down radio between MMCs or whatever else makes sense
    - Host is unaware of any device PM stuff
  - Device goes to sleep
    - Extended periods where device won’t respond
    - Host is aware and doesn’t schedule traffic
  - Device disconnects
    - Host is aware (explicit)

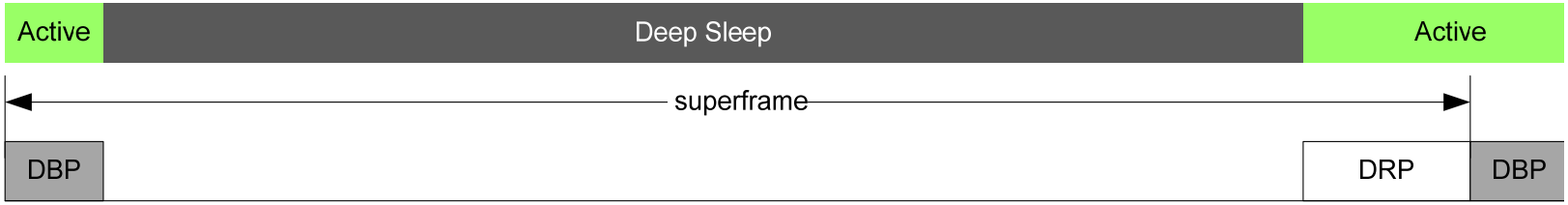
Power Management
Idle Workloads

Problematic workload: Low bandwidth (i.e. occasional data) async & int



- For “long” periods of no data, lots of lost opportunity to save power

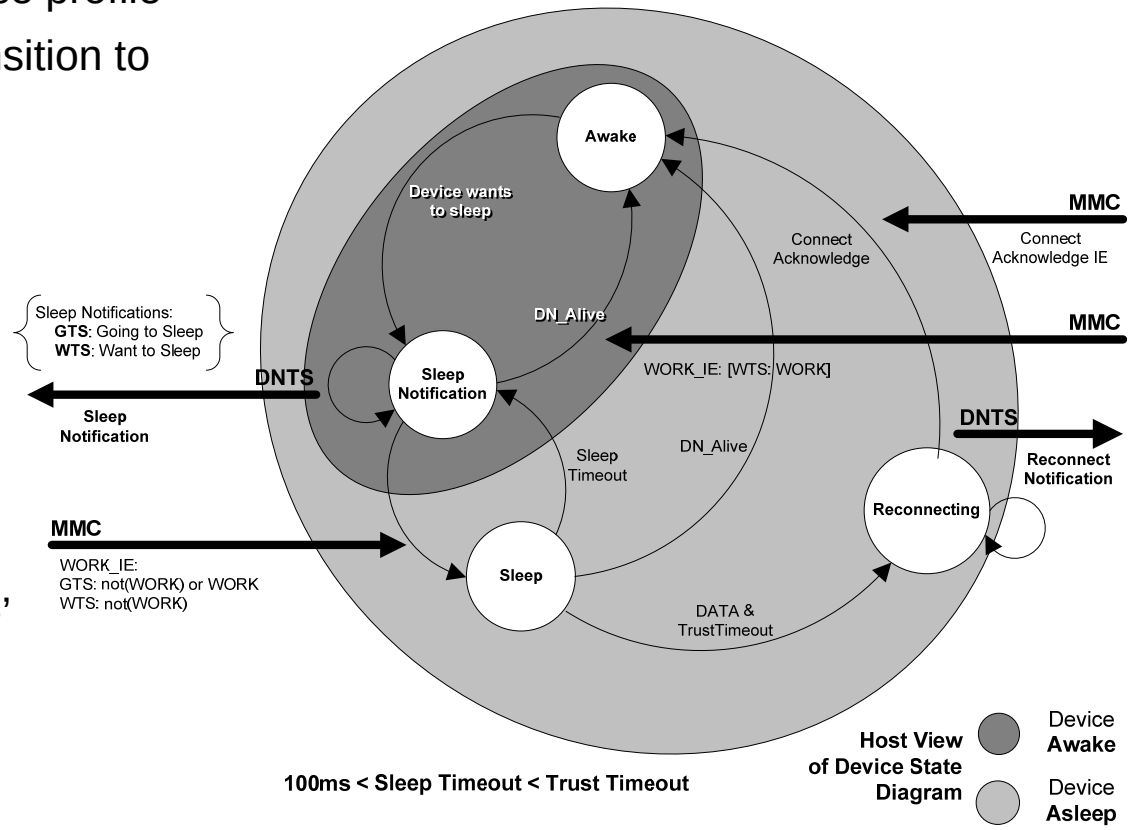
Would like to consider definition of mechanism(s) to allow host to change ‘polling’ profile (over time) to increase ‘deep-sleep’ time.



- Dialog between host and device to agree on ‘downshift’ and period
- Low-power interrupt is additional problem

Device/Host Sleep

- Encourage device implementations to aggressively utilize the sleep state
  - If devices aggressively sleep, then the host can have more opportunity to transition to a lower power use profile
  - Desire is to allow host to transition to sleep (often)
- Problem assertion: open, unbounded scan required by devices transitioning out of Sleep to re-acquire channel wastes power
  - How can we make this 'better' (under normal conditions) ?
    - Communicate a 'resume' aperture



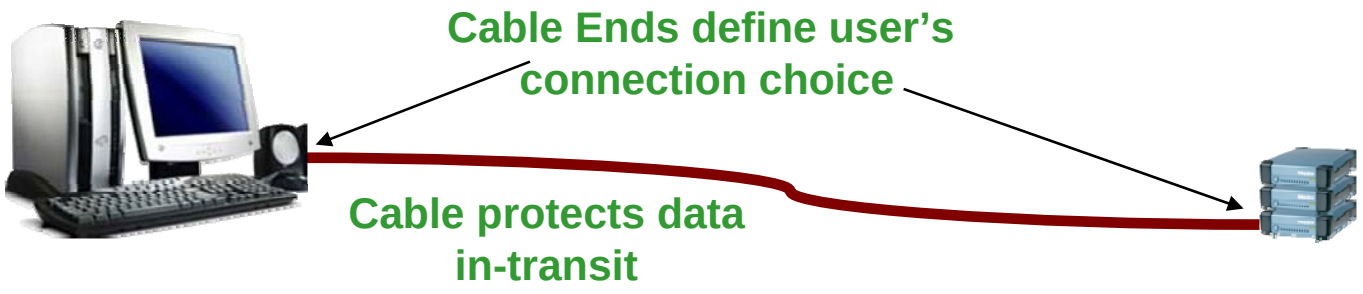
Power Management Problem Statement(s)

- Maximum ‘deep sleep’ residency of the host (and device) radio(s) per superframe
  - Add a mandatory device notification time slot at a fixed time in every superframe
- Controlled transition from ‘at rate’ polling of interrupt endpoints
  - Applies to Low-power Interrupts as well
- Provide a mechanism for remote wake-up capable devices to determine smaller ‘resume’ aperture
  - Mandate that hosts indicate to devices what their sleep cycle is

Power Profile Migration

Association and Security
Existing Methodology

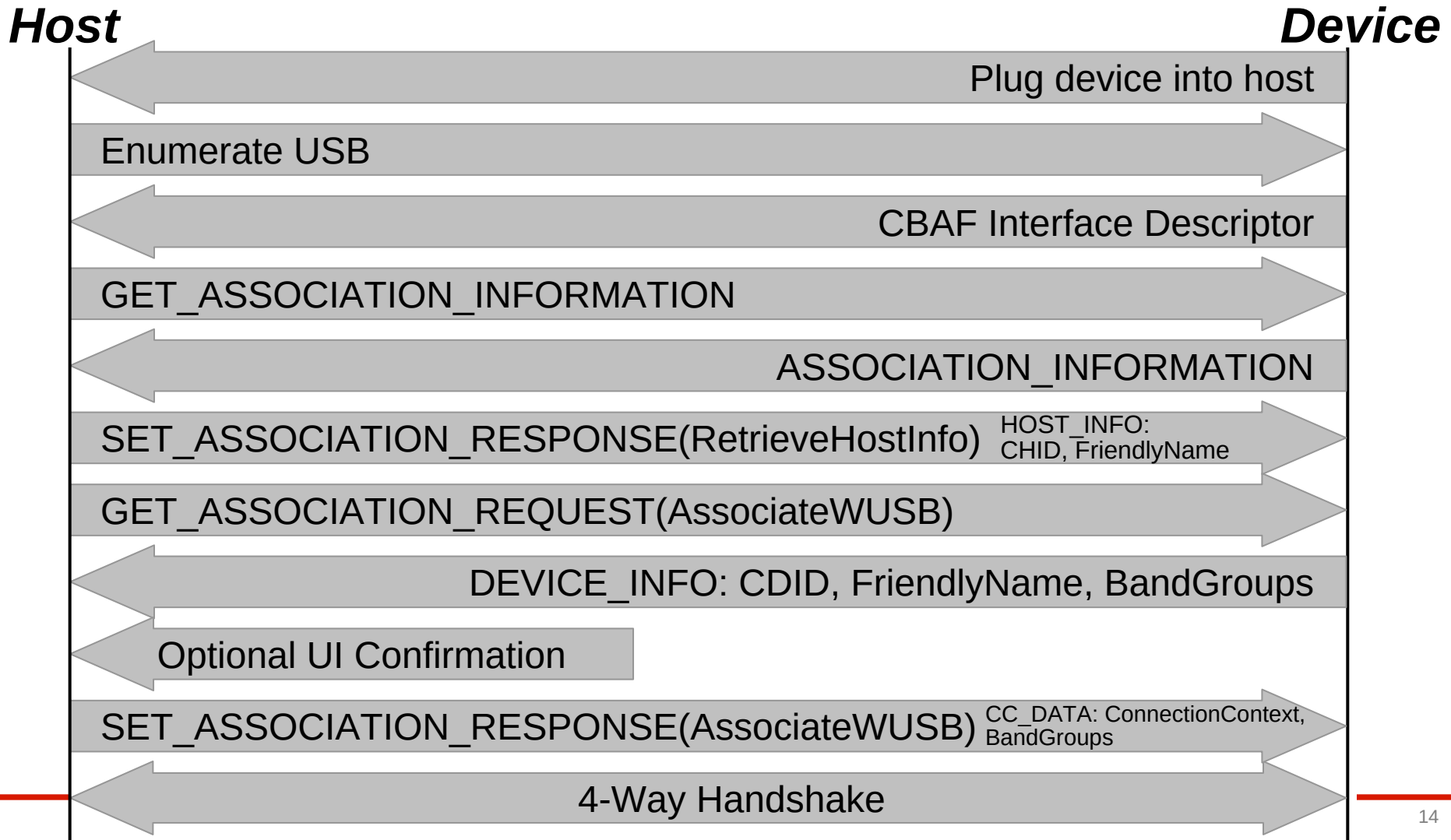
- Security's job:
  - Match the security afforded by the USB wire
  - Protect data in-transit
  - Encryption is required (AES-128 CCM)
- Association's job:
  - Connect the owner's devices the way the owner wants them connected



Association Models
Existing Methodology

- Two models: Cable and numeric
- Hosts must support cable and numeric
- Limited hosts/DRDs need only support TPL list
- Devices with USB ports must support cable model
- Devices with displays must support numeric model
- Devices must use at least one of the above

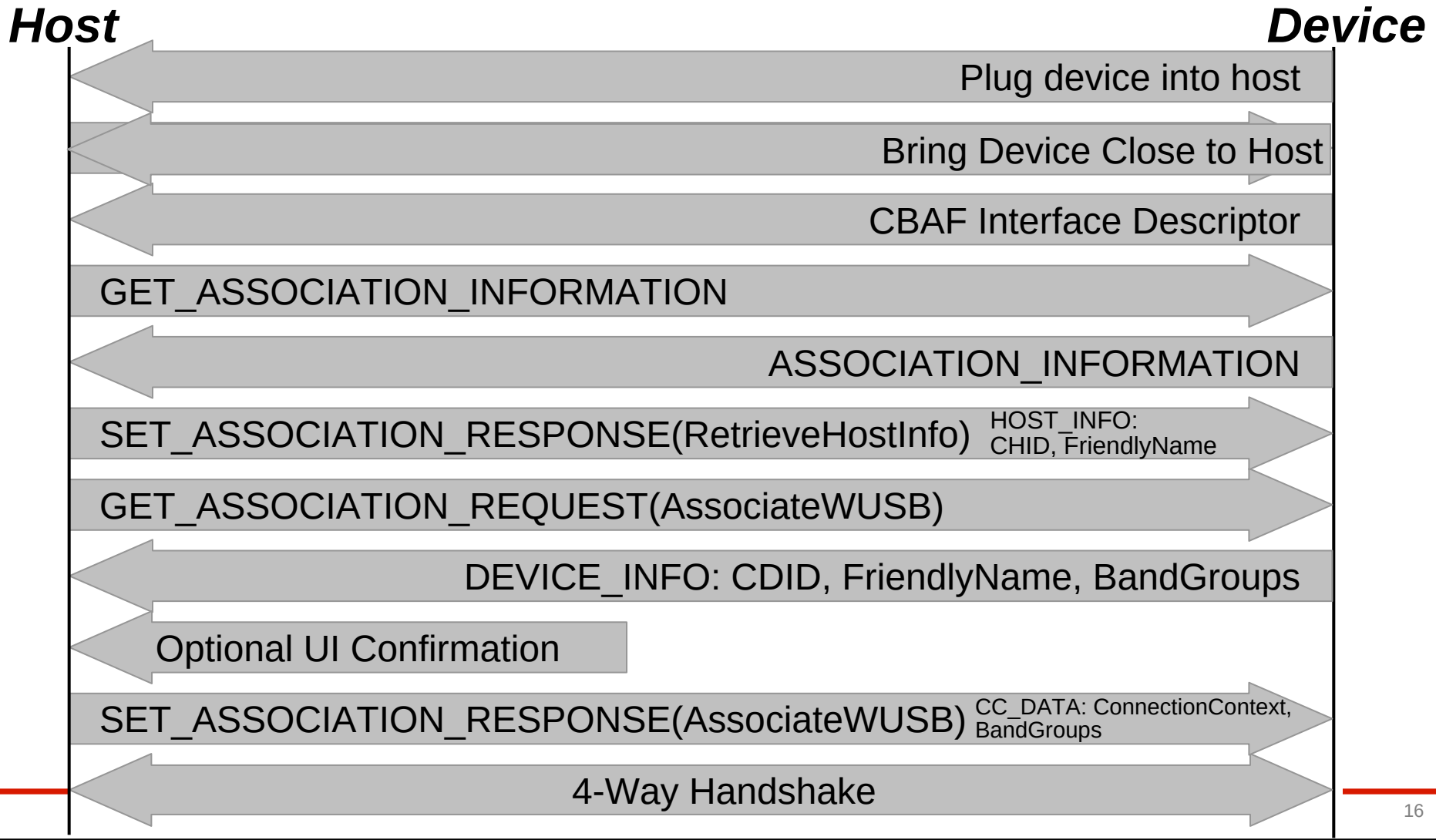
Cable Model
Existing Methodology



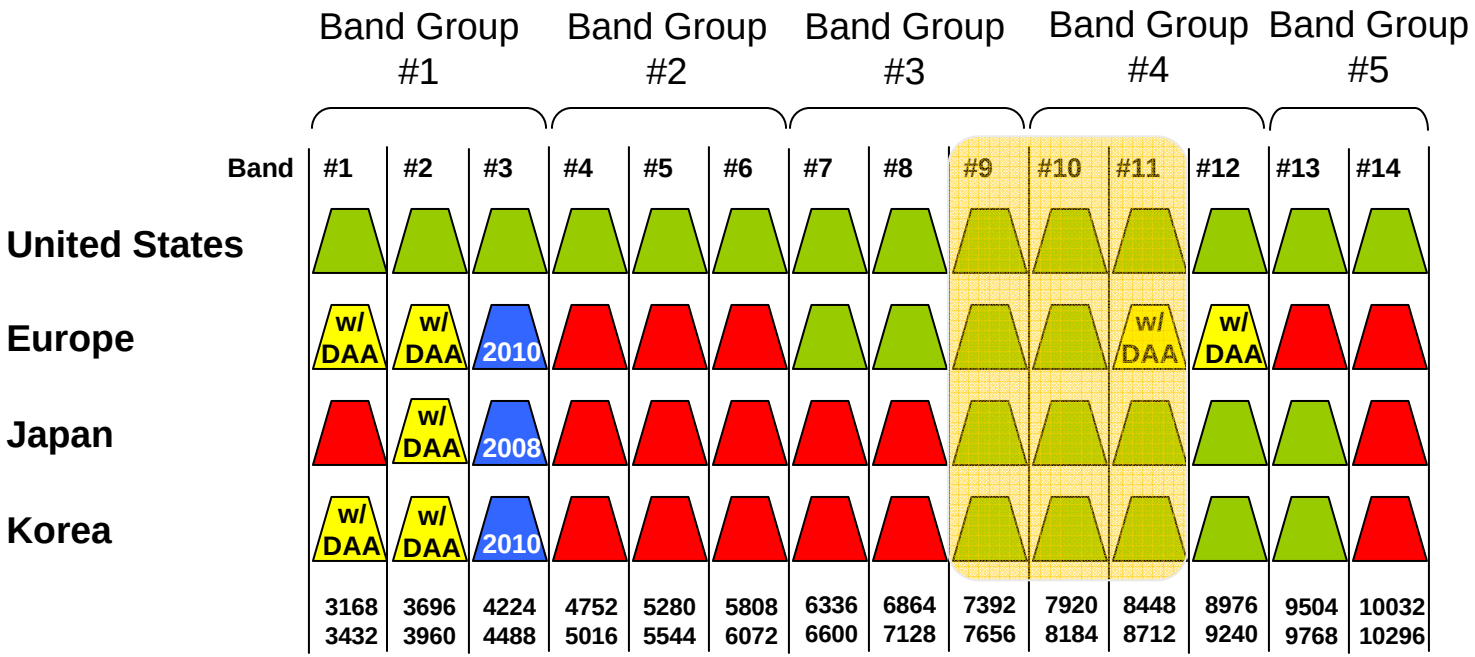
NFC for Wireless USB 1.1 Update

- NFC (Near Field Communication)
- Uses D-H algorithms to create shared secret
- Uses the cable model once secret is established
- NFC is not susceptible to Man in the Middle attack
- Hold device near host to associate
  - Connection context is passed

Association with NFC



UWB Upper Band Support



- Current Wireless USB devices use BG1
  - Has limitations in certain geographies
- BG6 has no such limitation

UWB Upper Band Support

- All full function Wireless USB hosts must support both BG1 and BG6
- Limited hosts can decide which band groups they support
- Host hops between BG1 and BG6
  - MMCs in each Band Group clearly indicate when the host will be back in the current Band Group
  - Issues with drift – the beacon periods may overlap
- Easiest implementation is to use two radios
  - This goes against the mantra of a single radio for multiple PALS

Summary

- Enhanced Power Management
- Easier than ever to Associate
- Supporting UWB Upper Bands

Wireless USB 1.1 specification completed 1H'08

Developers Conference 2007

Amsterdam, The Netherlands